Refine Search

Search Results -

Terms	Documents
L13 and L10	6

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: L14

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Saturday, April 16, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; THES=ASSIGNEE; PLUR=YES; OP=OR			
L14	L13 and l10	6	L14
L13	L12 and l3	6	L13
L12	L11 or l9	7580	L12
L11	380/201,202;705/58;713/191,193.ccls.	1762	L11
L10	L9 and l3	6	L10
L9	l8 or l7 or l6 or l5 or l4	6104	L9
L8	71/176,170,181.ccls.	0	L8
L7	713/202.ccls.	1145	L7
L6	709/229.ccls.	2328	L6
L5	705/44,54,57.ccls.	1029	L5
L4	380/28,30.ccls.	1785	L4
L3	L2 and @ad<=20001113	33	L3

L2	L1 and (encrypt$ with content)	121	L2
L1	(compar$ with hash$ with (number$ or value)) and ((updat$ or cop$) same content)	355	L1

END OF SEARCH HISTORY

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 6 of 6 returned.

☐ 1. Document ID: US 20030120604 A1

Using default format because multiple data bases are involved.

L14: Entry 1 of 6 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

US-CL-CURRENT: 705/57; 705/400, 705/50

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 2. Document ID: US 20020007452 A1

L14: Entry 2 of 6 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007452
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007452 A1

TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
TRAW, CHANDLER BRENDAN STANTON	PORTLAND	OR	US	
AUCSMITH, DAVID WAYNE	PORTLAND	OR	US	

US-CL-CURRENT: 713/152; 380/201, 705/57

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 3. Document ID: US 6859790 B1

L14: Entry 3 of 6 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 4. Document ID: US 6246767 B1

L14: Entry 4 of 6 File: USPT Jun 12, 2001

US-PAT-NO: 6246767
DOCUMENT-IDENTIFIER: US 6246767 B1
** See image for Certificate of Correction **

TITLE: Source authentication of download information in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 5. Document ID: US 6076077 A

L14: Entry 5 of 6 File: USPT Jun 13, 2000

US-PAT-NO: 6076077
DOCUMENT-IDENTIFIER: US 6076077 A
** See image for Certificate of Correction **

TITLE: Data management system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 6. Document ID: US 5666415 A

L14: Entry 6 of 6 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

Full | Title | Citation | Front | Review | Classification | Date | Reference | [illegible] | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L13 and L10	6

Display Format: - Change Format

Previous Page Next Page Go to Doc#

L14: Entry 2 of 6 File: PGPB Jan 17, 2002

DOCUMENT-IDENTIFIER: US 20020007452 A1
TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

Application Filing Date:
19970811

Current US Classification, US Secondary Class/Subclass:
380/201

Current US Classification, US Secondary Class/Subclass:
705/57

Detail Description Paragraph:
[0043] Following the completion of the preliminary authentication phase, an encrypted control channel is established between the authenticated devices. This preliminary control channel is used to initiate the transfer of protected content across the bus via encrypted content channels. The transfer of content is subject to immediate cancellation if any security threats are detected as the second, highly robust full authentication phase continues in the background.

Detail Description Paragraph:
[0077] When Device A is requested to initiate the transmission of protected content to Device B, Device A checks to see if an encrypted control channel has already been established between the two devices. If this control channel exists, the devices have already authenticated each other making further authentication unnecessary, and the devices can immediately establish an encrypted content channel. If however, the control channel does not exist, preliminary authentication must be initiated.

Detail Description Paragraph:
[0105] The control channel remains available as long as both devices remain powered up and attached to the communications link. The control channel can be repeatedly used to set up and manage the security of protected content streams without further authentication. Depending on the strength of the channel ciphers, it may be desirable to change the control channel keys on a regular basis. Control channel keys can be updated using a signed Diffie-Hellman key exchange similar to the one used during the full device authentication process. The computation for these key changes would typically be a low priority background activity, which would not affect overall device performance.

Detail Description Paragraph:
[0107] Content Channel Encryption

Detail Description Paragraph:
[0108] Exemplary embodiments of the present invention, to establish an encrypted channel for protected content, can utilize the following procedure once a secure control channel has been established by the preliminary or full device authentication procedures. Encryption of the control channel is performed to preserve the confidentiality of content channel keys and ensure the integrity of other messages. The source of the content sends a message via the encrypted control

channel to the compliant destination device (or devices in the case of a content multicast). This message contains: a randomly generated key which is unique for each stream of content. (K.sub.Content); the symmetric cipher to use (Content_Algo_Select); Cipher initialization state; the Isochronous channel associated with the content stream; Copy Control Information (such as CGMS bits); a sequence number initialized to the least significant 16 bits of A.sub.C and incremented for each additional message sent. Alternative embodiments of the present invention can forgo the inclusion of message elements such as the Cipher initialization state or the sequence number initialized to the least significant 16 bits of A.sub.C.

Detail Description Paragraph:
[0110] While content is flowing across an encrypted content channel, the copy control information associated with the stream can be updated at any time via the control channel(s) between the source device and destination device(s). Upon updating the copy control information, the key associated with the content channel should also be updated. In addition, depending on the strength of the channel ciphers, it may be desirable to change the content channel key on a periodic basis. New content channel keys and copy control information can be put into service when an indicator is transmitted over the content channel. This copy control information can be embedded in the content stream or as part of a header in the IEEE 1394 protocol, such as the CIP header.

Detail Description Paragraph:
[0123] A compliant device that transmits protected content must have a Channel Encryption Subsystem 606. Control messages, as well as protected content, are encrypted prior to transmission. Channel Encryption Subsystem 606 performs these encryptions. The keys used to encrypt the content and commands are passed to Channel Encryption Subsystem 606 from Authentication and Key Exchange Subsystem 604. Channel Encryption Subsystem 606 may support more than one cipher, although for interoperability it is preferable that a Baseline Cipher be supported. In a typical embodiment of the present invention, Authentication and Key Exchange Subsystem 604 specifies the particular cipher and key to be used for each packet transmitted.

Detail Description Paragraph:
[0135] Embodiments of the present invention provide a flexible system which can support a range of protection levels. Digital certificates enable device authentication which in turn facilitates the exclusion of devices which can circumvent the protection of the content. Furthermore, the content itself may be encrypted to ensure that even if it is copied, it will be in an unusable format. The present invention allows for a high level of content protection which can be implemented with a reasonable level of resources for consumer electronics equipment and computer systems.

CLAIMS:

1. A method of transferring content from a content source to a content sink, comprising: a) exchanging random challenges between the content source and the content sink; b) encrypting the exchanged random challenges with a secret key, then hashing the encrypted random challenges; c) exchanging the encrypted, hashed random challenges; d) comparing exchanged encrypted, hashed random challenges to expected values; e) establishing, if the exchanged encrypted, hashed random challenges match the expected values, a preliminary control channel; f) establishing a preliminary content channel; and g) transferring content over the preliminary content channel.

5. A method of transferring information, the method comprising: a) transmitting a first challenge from a first device to a second device, and transmitting a second challenge from the second device to the first device; b) in the first device, encrypting, then hashing the second challenge, and in the second device,

encrypting, then hashing the first challenge; c) transmitting the hashed, encrypted, second challenge to the second device, and transmitting the hashed, encrypted, first challenge to the first device; d) in the first device, comparing the hashed, encrypted first challenge to a first expected value, and in the second device comparing the hashed, encrypted second challenge to a second expected value; e) if both comparisons in step (d) result in a match, then establishing a preliminary content channel; and f) transferring information over the preliminary content channel.

Previous Doc Next Doc Go to Doc#

L14: Entry 3 of 6 File: USPT Feb 22, 2005

DOCUMENT-IDENTIFIER: US 6859790 B1
TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Application Filing Date (1):
20001018

Brief Summary Text (10):
For example, the CCI (Copy Control Information) and CGMS-A/D (Copy Generation Management System) being considered by the CPTWG (Copy Protection Technical Working Group) which is an operation organization of the copyright-related industry started to deal with DVD-ROM copyright protection issues, and the EMI-CCI (Encryption Mode Indicator-CCI) used with the 1394CP (Content Protection) which is a copyright protection measure for inter-equipment (home electronics) digital interfaces, but all of these end up simply changing the names of the SCMS copy control bits and continuing to use the same.

Brief Summary Text (14):
Now, rapid digitizing of broadcast networks, communication networks, and home electronics has necessitated the advent of high-level technology such as encryption technology and electronic watermarking technology, as a system to protect copyrights of digital contents. Further, the present state has reached a point which SCMS cannot deal with, even as a system to control copying.

Brief Summary Text (34):
To this end, the data distribution system according to the present invention comprises: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that arbitrary use including either one or both of recording and playing the contents data is to be permitted and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of the contents data of the generated distribution data, detects whether or not the use of the contents data is permitted, uses the contents data in the event that use thereof is permitted, and updates the use control information so as to decrease the number of permitted times of use based on the usage.

Brief Summary Text (35):
Also, the data distribution method according to the present invention: adds to desired contents data, in a manner wherein external operation is impossible; use control information containing information of the number of permitted times of use, which is the number of times that arbitrary use of the contents data including either one or both of recording and playing the contents data is to be permitted, and generates distribution data; distributes the distribution data to a desired distribution destination; detects whether or not the use of the contents data of the distribution data is permitted, based on the use control information of the distributed distribution data, at the distribution destination; uses the contents data in the event that use thereof is permitted as the result of the detection; and updates the use control information so as to decrease the number of permitted times of use according to the usage.

Brief Summary Text (36):
Also, the data processing device according to the present invention comprises: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of arbitrary use of the contents data including either one or both of recording and playing the contents data has been added to desired contents data, information of the number of permitted times of use from the use control information; use permitting means for detecting whether or not use of the content data is permitted, based on the extracted information of the number of permitted times of use; use control means for controlling the use so as to use the contents data in the event that use thereof is permitted as the result of the detection; using means for using the contents data based on the control; and control information updating means for updating the use control information so as to decrease the number of permitted times of use, based on the usage.

Brief Summary Text (37):
Also, the data use control device according to the present invention is provided to a device which uses the contents data of distribution data wherein use control information containing information of the number of times that arbitrary use of the contents data including either one or both of recording and playing the contents data is to be permitted, is added to desired contents data to be distributed; the data use control device comprising: control information extracting means for extracting, from the distributed distribution data, information of the number of permitted times of use of the use control information; use permitting means for detecting whether or not use of the content data is permitted, based on the extracted information of the number of permitted times of use; use control means for controlling use so as to use the contents data in the event that use thereof is permitted as the result of the detection; and control information updating means for updating the use control information so as to decrease the number of permitted times of use, based on the usage, in the event that the contents data is used.

Detailed Description Text (12):
The distribution key is sequentially validated and updated every certain period, such as once a month, and the key server 114 generates and stores several months worth of distributing keys, and transmits several months worth together to the contents provider 200, service provider 300, and user home networks 400.sub.-1 and 400.sub.-2.

Detailed Description Text (19):
The information of whether or not registration can be made indicates whether or not the contents can be used, and for example, in the event that there is a request for registration from equipment in the user home networks 400.sub.-1 and 400.sub.-2, the user registration database is searched, and depending on the recorded contents thereof, the equipment is registered or registration thereof is denied. This information of whether or not registration can be made is continuously updated, based on information such as whether there have been any unpaid bills or unauthorized processing, etc., provided from settlement firms such as banks and credit companies, the service provider 300, and so forth. Accordingly, the user administrative unit 118 denies registration of equipment having an ID which has been recorded to be registration not available, due to unpaid bills for example, and subsequently this equipment cannot use contents.

Detailed Description Text (167):
Then, the value obtained by passing the current value through the hash function once each time the user makes a copy is compared with the permitted number of generations, confirmation is made regarding whether or not this has exceeded the purchased number of tickets, and if not so, the copy action is permitted.

Current US Cross Reference Classification (4):

705/57

Current US Cross Reference Classification (8):
713/193

CLAIMS:

1. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted; and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage; wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control information containing said information of the number of permitted times of use that has been newly, and performs recording with said distribution data as a unit; and further comprising an administration device which is connected so as to be capable of communication with at least said data processing device, and which performs billing processing relating to the use of said contents data, based on information relating to use of said contents data sent from said data processing device; wherein said data processing device sends information relating to the use of said contents data to said administration device; wherein said data distributing device generates said distribution data by adding to said desired data information relating to the billing format whereby settlement can be made at said data processing device at the time of using said contents data, as said use control information; wherein said data processing device determines the billing format for use of said contents data, based on said information relating to billing format from said use control information of said distribution data; wherein said data processing device sends information relating to the determined billing format to said administration device; and wherein said administration device performs billing processing relating to use of said contents data, based on said information relating to billing format sent from said data processing device.

2. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted; and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage; wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control

information containing said information of the number of permitted times of use that has been newly set, and performs recording with said distribution data as a unit; and wherein said data processing device sends information relating to the number of times of use of said contents data to said administration device; and wherein said administration device performs billing processing, based on said information relating to the number of times of use of said contents data that is sent.

3. A data distribution system, comprising: a data distributing device which adds to desired contents data which is the object of distribution use control information containing information of the number of permitted times of use, which is the number of times that use including either one or both of recording and playing said contents data is to be permitted; and generates distribution data; and a data processing device which, based on the information of the number of permitted times of use of said contents data of said generated distribution data, detects whether or not the use of said contents data is permitted, uses said contents data in the event that use thereof is permitted, and updates said use control information so as to decrease said number of permitted times of use based on said usage wherein said data processing device comprises a signal processing device wherein external observation and alteration of the signal processing state is impossible, and wherein said signal processing device performs detection of whether or not use of said contents data is permitted; control of use of said contents data based on said detection results, and updating of said use control information based on said use; wherein in the event of recording said contents data, said data processing device generates new distribution data by adding to said contents data said use control information containing said information of the number of permitted times of use that has been newly, and performs recording with said distribution data as a unit; and further comprising an administration device which is connected so as to be capable of communication with at least said data processing device, and which performs billing processing relating to the use of said contents data, based on information relating to use of said contents data sent from said data processing device; wherein said data processing device sends information relating to the use of said contents data to said administration device; wherein said data distributing device generates said distribution data containing information of number of permitted times of use represented by a hash value obtained by passing a predetermined initial value through a hash function a number of times equal to the number of times that use is permitted; and information of the essential number of times of use represented by said predetermined initial value as use control information; and wherein said data processing device restricts use of said distribution data in the event that the hash value indicating the maximum number of times of use allowed and the hash value indicating the number of times of essential use become the same.

5. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends

information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said distribution data contains information relating to the billing format for said contents data within said use control information; and wherein the billing format for use of said contents data is determined at said distribution destination, based on said information relating to the billing format of said use control information for said distribution data.

9. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said billing is not performed for the first recording after distribution of said distribution data.

10. A data distribution method, which: adds to desired contents data, in a manner wherein external operation is impossible, use control information containing information of the number of permitted times of use, which is the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, and generates distribution data; distributes said distribution data to a desired distribution destination; detects whether or not the use of said contents data of said distribution data is permitted, based on said use control information of said distributed distribution data, at said distribution destination; uses said contents data in the event that use thereof is permitted as the result of said detection; and updates said use control information so as to decrease said number of permitted times of use according to said usage; wherein detection of whether or not use of said contents data is permitted, control of use of said contents data based on said detection results, and updating of said use control information based on said use, are performed within a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein in the event that said contents data has been used, said distribution destination sends information relating to use of said contents data to a predetermined administration device; wherein said administration device performs billing processing relating to use of said contents data, based on said generated information relating to use of

said contents data; and wherein in the event of using said contents data by recording, this is performed by using as a unit; said distribution data containing said contents data and said use control information containing said information of the number of permitted times of use that has been newly set; wherein said distribution data contains information of the number of times use has been permitted and the number of times essentially already used, as said use control information, with a hash value of a hash function; and wherein detection of whether or not use of said distribution data is permitted, and updating of information indicating the number of times said distribution data has already been essentially used based on use of said distribution data, are performed by comparing information of said number of permitted times of use with information of number of times already used, at said distribution destination.

13. A data processing device, comprising: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of use of said contents data including either one or both of recording and playing said contents data has been added to desired contents data, information of the number of permitted times of use from said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling said use so as to use said contents data in the event that use thereof is permitted as the result of said detection; using means for using said contents data based on said control; and control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage; wherein said control information extracting means, said use permitting means, said use control means, and said control information updating means are configured of a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said using means so as to play said contents data in the event that playing thereof is permitted as the result of said detection; wherein said using means plays said contents data based on said control; and wherein said control information updating means updates said use control information based on said playing; and further comprising distribution data generating means for adding use control information containing said information of the number of permitted times of use that has been newly set to a predetermined value to said contents data, thereby generating new distribution data; wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said distribution data generating means and said using means so as to record said contents data in the event that recording thereof is permitted as the result of said detection; wherein said distribution data generating means generates new distribution data using said contents data which is the object of recording; wherein said using means records new distribution data generated based on said control; and wherein said control information updating means updates said use control information based on said new generation of distribution data and said recording.

14. A data processing device according to claim 13, wherein said distribution data contains information of number of permitted times of use by recording of said distribution data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said information of the number of permitted times of use by recording of said distribution data at the recording originating side; and wherein said distribution data generating means sets the number of permitted times of use by said recording of the generated distribution data, based on said information of the number of permitted times of use by recording of said distribution data at said recording originating side; and wherein said using means records new distribution data generated; and wherein said

control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by recording set to said recorded distribution data.

15. A data processing device according to claim 13, wherein said distribution data separately comprises information of number of permitted times of using said distribution data as original data for recording, and information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on information of the number of permitted times of use by recording of said distribution data as original data; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said using means records said generated new distribution data; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by said recording set to said recorded distribution data.

20. A data processing device according to claim 13, wherein, in the event of using said contents data by recording; said distribution data generating means generates said distribution data containing said use control information containing information wherein the number of permitted times of use of said contents data is set to a predetermined value smaller than the number of permitted times of use by recording of the original distribution data; said using means records said newly generated distribution data; and said control information updating means updates the information of the number of permitted times of use by recording for the original distribution data, based on recording of said new distribution data and the number of permitted times of use by recording set to said new distribution data.

21. A data processing device according to claim 16, wherein, in the event of newly increasing the number of permitted times of use of said distribution data which has already been distributed, said communication means transmits information to said administration device for requesting a desired number of times of use of said contents data, and receives a response to said request from said administration device; and wherein in the event that said received response is such that permits said request, said control information updating means increases the number of permitted times of use of said distribution data which has already been distributed by the maximum number of times allowed.

25. A data processing device, comprising: control information extracting means for extracting, from distribution data wherein use control information containing information of the number of permitted times of use of said contents data including either one or both of recording and playing said contents data has been added to desired contents data, information of the number of permitted times of use from said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling said use so as to use said contents data in the event that use thereof is permitted as the result of said detection; using means for using said contents data based on said control; and control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage; wherein said control information extracting means, said use permitting means, said use control means, and said control information updating means are configured of a signal processing device regarding which external observation and alteration of the signal processing state is impossible; wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means

controls said using means so as to play said contents data in the event that playing thereof is permitted as the result of said detection; wherein said using means plays said contents data based on said control; and wherein said control information updating means updates said use control information based on said playing; and further comprising display means for displaying arbitrary information of said use control information of said distributed distribution data, and information based on said information.

26. A data use control device provided to a device which uses said contents data of distribution data wherein use control information containing information of the number of times that use of said contents data including either one or both of recording and playing said contents data is to be permitted, is added to desired contents data to be distributed; said data use control device comprising: control information extracting means for extracting, from said distributed distribution data, information of the number of permitted times of use of said use control information; use permitting means for detecting whether or not use of said content data is permitted, based on said extracted information of the number of permitted times of use; use control means for controlling use so as to use said contents data in the event that use thereof is permitted as the result of said detection; control information updating means for updating said use control information so as to decrease said number of permitted times of use, based on said usage, in the event that said contents data is used; and a signal processing device regarding which external observation and alteration of the signal processing state is impossible: wherein said use permitting means detects whether or not playing of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said use so as to play said contents data in the event that playing thereof is permitted as the result of said detection; and wherein said control information updating means updates said use control information based on said playing; and further comprising distribution data generating means for adding use control information containing said information of the number of permitted times of use that has been newly set to a predetermined value to said contents data, thereby generating new distribution data; wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said extracted information of the number of permitted times of use; wherein said use control means controls said distribution data generating means so as to record said contents data in the event that recording thereof is permitted as the result of said detection; wherein said distribution data generating means generates said new distribution data using said contents data which is the object of recording; and wherein said control information updating means updates said use control information based on said new generation of distribution data and said recording.

27. A data use control device according to claim 26, wherein said distribution data contains information of the number of permitted times of use by recording of said distribution data; and wherein said use permitting means detects whether or not recording of said contents data is permitted, based on said information of the number of permitted times of use by recording of said distribution data at the recording originating side; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of the number of permitted times of use by said recording of said distribution data at said recording originating side; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by recording set to said recorded distribution data.

28. A data use control device according to claim 26, wherein said distribution data separately comprises information of number of permitted times of using said distribution data as original data for recording, and information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said use permitting

means detects whether or not recording of said contents data is permitted, based on information of the number of permitted times of use by recording of said distribution data as original data; and wherein said distribution data generating means sets the number of permitted times of use by recording of the generated distribution data, based on information of number of permitted times of using by recording for setting said distribution data as distribution data for recording as original data; and wherein said control information updating means updates said use control information based on the recording of said distribution data, and the number of permitted times of use by said recording set to said recorded distribution data.

33. A data use control device according to claim 26, wherein, in the event of using said contents data by recording; said distribution data generating means generates said distribution data containing said use control information containing information wherein the number of permitted times of use of contents data is set to a predetermined value smaller than the number of permitted times of use by recording of the original distribution data; and said control information updating means updates the information of the number of permitted times of use by recording for the original distribution data, based on recording of said new distribution data and the number of permitted times of use by recording set to said new distribution data.

34. A data use control device according to claim 32, wherein, in the event of newly increasing the number of permitted times of use of said distribution data which has already been distributed, said communication control means transmits information to said administration device for requesting a desired number of times of use of said contents data, and receives a response to said request from said administration device; and wherein in the event that said received response is such that permits said request, said control information updating means increases the number of permitted times of use of said distribution data which has already been distributed by the maximum number of times allowed.

Previous Doc Next Doc Go to Doc#

L14: Entry 1 of 6 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
SONY CORPORATION				03

APPL-NO: 09/ 534744 [PALM]
DATE FILED: March 24, 2000

CONTINUED PROSECUTION APPLICATION: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	DOC-ID	APPL-DATE
JP	11-084918	1999JP-11-084918	March 26, 1999
JP	11-183411	1999JP-11-183411	June 29, 1999
JP	2000-023329	2000JP-2000-023329	January 27, 2000

INT-CL: [07] G06 F 17/60

US-CL-PUBLISHED: 705/57; 705/400, 705/50
US-CL-CURRENT: 705/57; 705/400, 705/50

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A reproducing apparatus for reproducing data from a record medium having a program area and a management area, the program area being used for recording a plurality of files, the management area being used for managing forging prohibition information against a particular file recorded in the program area is disclosed,

the apparatus comprising a calculating means for calculating the forging prohibition information managed in the management area of the record medium whenever a file recorded in the recorde medium is reproduced, a comparing means for comparing a value calculated by the calculating means corresponding to a former reproduction command with a value calculated by the calculating means corresponding to a current reproduction command, and a controlling means for permitting the file corresponding to the current reproduction command to be reproduced when the value calculated corresponding to the former reproduction command is the same as the value calculated corresponding to the current reproduction command as the result of the comparing means.

Previous Doc Next Doc Go to Doc#

L14: Entry 2 of 6 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007452
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007452 A1

TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
TRAW, CHANDLER BRENDAN STANTON	PORTLAND	OR	US	
AUCSMITH, DAVID WAYNE	PORTLAND	OR	US	

APPL-NO: 08/ 909338 [PALM]
DATE FILED: August 11, 1997

CONTINUED PROSECUTION APPLICATION: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

RELATED-US-APPL-DATA:
Application 08/909338 is a continuation-in-part-of US application 08/791245, filed January 30, 1997, US Patent No. 5949877

INT-CL: [07] H04 L 9/00, H04 N 7/167

US-CL-PUBLISHED: 713/152; 380/201, 705/57
US-CL-CURRENT: 713/152; 380/201, 705/57

REPRESENTATIVE-FIGURES: 3A,3B

ABSTRACT:

A method for protecting digital content from copying and/or other misuse as it is transferred between one or more computationally constrained devices over insecure links, includes preliminarily authenticating that both a content source and a content sink are compliant devices, and transferring content between compliant devices. In a further aspect of the invention, in the background, concurrently with the transfer of content, at least a second cryptographic process is performed.

In an embodiment, establishing a preliminary control channel includes exchanging random challenges between devices, encrypting, under a shared secret key, and hashing the exchanged random challenges, exchanging the results of the encryption and hash functions and then verifying that the appropriate results have been generated.

CROSS REFERENCE TO RELATED APPLICATIONS

L14: Entry 3 of 6 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

DATE-ISSUED: February 22, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Nonaka; Akira	Kanagawa			JP
Ezaki; Tadashi	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Sony Corporation	Tokyo			JP	03

APPL-NO: 09/ 691410 [PALM]
DATE FILED: October 18, 2000

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	11-298921	October 20, 1999

INT-CL: [07] G06T01760

US-CL-ISSUED: 705/51; 705/1, 705/51, 705/55, 705/57, 380/3, 380/4, 380/255, 707/9, 707/65, 713/189, 713/193, 713/194
US-CL-CURRENT: 705/51; 380/255, 705/1, 705/55, 705/57, 705/65, 707/9, 713/189, 713/193, 713/194

FIELD-OF-SEARCH: 705/51, 705/1, 705/55, 705/57, 380/3, 380/4, 380/255, 707/65, 707/9, 713/189, 713/193, 713/194

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5715403	February 1998	Stefik	705/44
☐	5825883	October 1998	Archibald et al.	705/53

☐	6016509	January 2000	Dedrick	709/224
☐	6233684	May 2001	Stefik et al.	713/176
☐	6289455	September 2001	Kocher et al.	713/194
☐	6341273	January 2002	Briscoe	705/41

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
2002230428	August 2002	JP	

OTHER PUBLICATIONS

http://www.vector-networks.com/pcduo-enterprise/datasheets/ Software_Metering.pdf.

ART-UNIT: 3621

PRIMARY-EXAMINER: Trammell; James P.

ASSISTANT-EXAMINER: Winter; J

ATTY-AGENT-FIRM: Frommer Lawrence & Haug LLP Frommer; William S.

ABSTRACT:

A contents provider stores contents data in a container in a format which can only be decoded with a key distributed from an EMD service center, and transmits the container to a service provider. The service provider adds pricing information and the like and distributes this to a user home network. The user home network pays charges to the EMD service center based on the pricing information, receives the key, and decodes the contents data. Information regarding the number of times which copying is permitted is contained in the secure container, and the number of times permitted is increased each time charges are paid, thereby enabling copying to other media and the like. It is impossible to make copies from a container simply copied, or in cases where in the number of permitted times of copies has been used up. Thus, contents data can be distributed in a format wherein copying of contents data can be controlled including the number of copies made.

36 Claims, 34 Drawing figures

Previous Doc Next Doc Go to Doc#

L14: Entry 4 of 6 File: USPT Jun 12, 2001

US-PAT-NO: 6246767
DOCUMENT-IDENTIFIER: US 6246767 B1
**** See image for Certificate of Correction ****

TITLE: Source authentication of download information in a conditional access system

DATE-ISSUED: June 12, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Akins, III; Glendon L.	Gainesville	GA		
Banker; Robert O.	Cumming	GA		
Palgon; Michael S.	Atlanta	GA		
Pinder; Howard G.	Norcross	GA		
Wasilewski; Anthony J.	Alpharetta	GA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Scientific-Atlanta, Inc.	Lawrenceville	GA			02

APPL-NO: 09/ 488104 [PALM]
DATE FILED: January 20, 2000

PARENT-CASE:
RELATED PATENT APPLICATIONS This Application is a Continuation of App. No. 09/127,152, filed Jul. 31, 1998, now abandoned, which claims the benefit of U.S. Provisional Application No. 60/054,575, filed Aug. 1, 1997, and is a CIP of Application Ser. No. 09/111,958, filed Jul. 8, 1998, now abandoned, which claims the benefit of U.S. Provisional Application No. 60/054,578, filed Aug. 1, 1997, and is CIP of application Ser. No. 08/767,535, filed Dec. 16, 1996, U.S. Pat. No. 6,005,938, and is a CIP of application Ser. No. 08/580,759 filed Dec. 29, 1995, U.S. Pat. No. 5,870,474, which claims the benefit of U.S. Provisional Application No. 60/007,962, filed Dec. 4, 1995, and is CIP of application Ser. No. 08/415,617, filed Apr. 3, 1995, U.S. Pat. No. 5,742,677.

INT-CL: [07] H04 N 7/167

US-CL-ISSUED: 380/21; 380/232, 380/43, 380/285, 380/282, 380/30, 713/153, 713/168
US-CL-CURRENT: 380/210; 380/232, 380/282, 380/285, 380/30, 380/43, 713/153, 713/168

FIELD-OF-SEARCH: 380/232, 380/43, 380/285, 380/282, 380/30, 713/168, 713/153

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4993068	February 1991	Piosenka et al.	380/23
☐	5740246	April 1998	Saito	380/21
☐	5787172	July 1998	Arnold	380/21

ART-UNIT: 212

PRIMARY-EXAMINER: Peeso; Thomas R.

ASSISTANT-EXAMINER: Jack; Todd

ATTY-AGENT-FIRM: West; John Eric Massaroni; Kenneth M. Gardner; Kelly A.

ABSTRACT:

A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

36 Claims, 30 Drawing figures

Previous Doc Next Doc Go to Doc#

L14: Entry 5 of 6 File: USPT Jun 13, 2000

US-PAT-NO: 6076077
DOCUMENT-IDENTIFIER: US 6076077 A
**** See image for Certificate of Correction ****

TITLE: Data management system

DATE-ISSUED: June 13, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Saito; Makoto	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Mitsubishi Corporation	Tokyo			JP	03

APPL-NO: 08/ 846661 [PALM]
DATE FILED: May 1, 1997

PARENT-CASE:
CROSS-REFERENCE TO RELATED APPLICATIONS This is a continuation-in-part of prior U.S. patent application Ser. No. 08/549,271 filed on Oct. 27, 1995, now U.S. Pat. No. 5,646,999, and prior U.S. patent application Ser. No. 08/733,504 filed on Oct. 18, 1996, now U.S. Pat. No. 5,974,141 all of which are commonly assigned to the assignee of the present invention.

INT-CL: [07] H04 L 9/08, H04 L 9/14, H04 K 1/00

US-CL-ISSUED: 705/51; 380/201, 380/278, 380/279, 713/167, 713/193, 705/52, 705/59, 705/54, 705/57
US-CL-CURRENT: 705/51; 380/201, 380/278, 380/279, 705/52, 705/54, 705/57, 705/59, 713/167, 713/193

FIELD-OF-SEARCH: 380/4, 380/49, 380/21, 380/201, 380/278, 380/279, 713/167, 713/193, 705/51, 705/52, 705/54, 705/57, 705/59

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5465299	November 1995	Matsumoto et al.	380/23

ART-UNIT: 276

PRIMARY-EXAMINER: Laufer; Pinchus M.

ASSISTANT-EXAMINER: Sayadian; Hrayr A.

ATTY-AGENT-FIRM: Armstrong, Westerman, Hattori, McLeland & Naughton

ABSTRACT:

A system for dealing in an original data content and an edited data content. A data content is handled as an object, and the data content is edited by editing a data content, functioning as an object, in accordance with an edit program. The edited data content is expressed by the original data content and the editing scenario which describes editing detail by the edit program. Only the encrypted editing scenario is dealt in. Upon receipt of the encrypted editing scenario, a user decrypts the encrypted editing scenario using a crypt key obtained from a key management center, and obtains the original data content from the database in accordance with the editing scenario and re-constitutes the edited data content. In case there is the one who wishes sale of the editing scenario, its utilization right is sold by auction.

4 Claims, 7 Drawing figures

Previous Doc Next Doc Go to Doc#

L14: Entry 6 of 6 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

DATE-ISSUED: September 9, 1997

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kaufman; Charles William	Northboro	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Digital Equipment Corporation	Maynard	MA			02

APPL-NO: 08/ 508766 [PALM]
DATE FILED: July 28, 1995

INT-CL: [06] H04 K 1/00

US-CL-ISSUED: 380/23; 380/25, 380/30, 380/28, 380/21, 380/49
US-CL-CURRENT: 713/159; 380/28, 380/30, 713/172

FIELD-OF-SEARCH: 380/23, 380/24, 380/25, 380/30, 380/28, 380/21, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5260070	November 1993	Ohta	395/425
☐	5347580	September 1994	Molva et al.	380/25
☐	5369705	November 1994	Bird et al.	380/21
☐	5371794	December 1994	Diffie et al.	380/21
☐	5418854	May 1995	Kaufman et al.	380/23
☐	5491750	February 1996	Bellare et al.	380/21
☐	5497421	March 1996	Kaufman et al.	380/23
☐	5515439	May 1996	Bantz et al.	380/23

ART-UNIT: 222

PRIMARY-EXAMINER: Cain; David C.

ABSTRACT:

Method for providing user authentication and a memory for storing a computer program for providing user authentication are described. The method includes the steps of providing a first argument including a one-way cryptographic transformation of a password and a second argument including a one-way cryptographic transformation of a cryptographic combination of the password and a first nonce, computing a first term using the first argument and computing a second term using the first nonce, and comparing the second term with the second argument. The memory storing a computer program, the computer program including, means for providing a first argument including a one-way cryptographic transformation of a password and a second argument including a one-way cryptographic transformation of a cryptographic combination of the password and a first nonce, means for computing a first term using the first argument and computing a second term using the first nonce, and means for comparing the second term with the second argument.

20 Claims, 7 Drawing figures

Previous Doc Next Doc Go to Doc#

L14: Entry 6 of 6 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

DATE-ISSUED: September 9, 1997

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kaufman; Charles William	Northboro	MA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Digital Equipment Corporation	Maynard	MA			02

APPL-NO: 08/ 508766 [PALM]
DATE FILED: July 28, 1995

INT-CL: [06] H04 K 1/00

US-CL-ISSUED: 380/23; 380/25, 380/30, 380/28, 380/21, 380/49
US-CL-CURRENT: 713/159; 380/28, 380/30, 713/172

FIELD-OF-SEARCH: 380/23, 380/24, 380/25, 380/30, 380/28, 380/21, 380/49

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5260070	November 1993	Ohta	395/425
☐	5347580	September 1994	Molva et al.	380/25
☐	5369705	November 1994	Bird et al.	380/21
☐	5371794	December 1994	Diffie et al.	380/21
☐	5418854	May 1995	Kaufman et al.	380/23
☐	5491750	February 1996	Bellare et al.	380/21
☐	5497421	March 1996	Kaufman et al.	380/23
☐	5515439	May 1996	Bantz et al.	380/23

ART-UNIT: 222

PRIMARY-EXAMINER: Cain; David C.

ABSTRACT:

Method for providing user authentication and a memory for storing a computer program for providing user authentication are described. The method includes the steps of providing a first argument including a one-way cryptographic transformation of a password and a second argument including a one-way cryptographic transformation of a cryptographic combination of the password and a first nonce, computing a first term using the first argument and computing a second term using the first nonce, and comparing the second term with the second argument. The memory storing a computer program, the computer program including, means for providing a first argument including a one-way cryptographic transformation of a password and a second argument including a one-way cryptographic transformation of a cryptographic combination of the password and a first nonce, means for computing a first term using the first argument and computing a second term using the first nonce, and means for comparing the second term with the second argument.

20 Claims, 7 Drawing figures

Previous Doc Next Doc Go to Doc#

9/711747

L14: Entry 1 of 6 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	COUNTRY	TYPE CODE
SONY CORPORATION				03

APPL-NO: 09/ 534744 [PALM]
DATE FILED: March 24, 2000

CONTINUED PROSECUTION APPLICATION: This is a publication of a continued prosecution application (CPA) filed under 37 CFR 1.53(d).

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	DOC-ID	APPL-DATE
JP	11-084918	1999JP-11-084918	March 26, 1999
JP	11-183411	1999JP-11-183411	June 29, 1999
JP	2000-023329	2000JP-2000-023329	January 27, 2000

INT-CL: [07] G06 F 17/60

US-CL-PUBLISHED: 705/57; 705/400, 705/50
US-CL-CURRENT: 705/57; 705/400, 705/50

REPRESENTATIVE-FIGURES: 1

ABSTRACT:

A reproducing apparatus for reproducing data from a record medium having a program area and a management area, the program area being used for recording a plurality of files, the management area being used for managing forging prohibition information against a particular file recorded in the program area is disclosed,

the apparatus comprising a calculating means for calculating the forging prohibition information managed in the management area of the record medium whenever a file recorded in the recorde medium is reproduced, a comparing means for comparing a value calculated by the calculating means corresponding to a former reproduction command with a value calculated by the calculating means corresponding to a current reproduction command, and a controlling means for permitting the file corresponding to the current reproduction command to be reproduced when the value calculated corresponding to the former reproduction command is the same as the value calculated corresponding to the current reproduction command as the result of the comparing means.

Previous Doc Next Doc Go to Doc#

L14: Entry 1 of 6 File: PGPB Jun 26, 2003

DOCUMENT-IDENTIFIER: US 20030120604 A1
TITLE: Reproducing apparatus and reproducing method

Application Filing Date:
20000324

Current US Classification, US Primary Class/Subclass:
705/57

Detail Description Paragraph:
[0061] The encoder/decoder block 12 of the audio encoder/decoder IC 10 supplies encoded data to a DES encrypting circuit 22 through an interface 21 of the security IC 20. The DES encrypting circuit 22 has a FIFO 23. The DES encrypting circuit 22 is disposed so as to protect the copyright of contents. The memory card 40 also has a DES encrypting circuit. The DES encrypting circuit 22 of the recording/reproducing apparatus has a plurality of master keys and an apparatus-unique storage key. The DES encrypting circuit 22 also has a random number generating circuit. The DES encrypting circuit 22 can share an authenticating process and a session key with the memory card 40 that has the DES encrypting circuit. In addition, the DES encrypting circuit 22 can re-encrypt data with the storage key of the DES encrypting circuit.

Detail Description Paragraph:
[0077] The security block 52 of the memory card 40 has a plurality of authentication keys and a unique storage key for each memory card. The nonvolatile memory 55 stores a key necessary for encrypting data. The key stored in the nonvolatile memory 55 cannot be analyzed. According to the embodiment, for example, a storage key is stored in the nonvolatile memory 55. The security block 52 also has a random number generating circuit. The security block 52 authenticates an applicable recorder/player and shares a session key therewith. In addition, the security block 52 re-encrypts contents with the storage key through the DSE encrypting circuit 54.

Detail Description Paragraph:
[0079] When contents are written to the memory card 40, the recorder/player encrypts a contents key with a session key and supplies the encrypted data to the memory card 40. The memory card 40 decrypts the contents key with the session key, re-encrypts the contents key with a storage key, and supplies the contents key to the recorder/player. The storage key is a unique key for each memory card 40. When the recorder/player receives the encrypted contents key, the recorder/player performs a formatting process for the encrypted contents key, and writes the encrypted contents key and the encrypted contents to the memory card 40.

Detail Description Paragraph:
[0081] When data is read from the memory card 40, the contents key encrypted with the storage key and the contents encrypted with the block key are read from the flash memory 42. The security block 52 decrypts the contents key with the storage key. The security block 52 re-encrypts the decrypted content key with the session key and transmits the re-encrypted contents key to the recorder/player. The recorder/player decrypts the contents key with the received session key and

generates a block key with the decrypted contents key. The recorder/player successively decrypts the encrypted ATRAC3 data.

Detail Description Paragraph:
[0085] One page is composed of a data portion of 512 bytes and a redundant portion of 16 bytes. The first three bytes of the redundant portion is an overwrite portion that is rewritten whenever data is updated. The first three bytes successively contain a block status area, a page status area, and an update status area. The remaining 13 bytes of the redundant portion are fixed data that depends on the contents of the data portion. The 13 bytes contain a management flag area (1 byte), a logical address area (2 bytes), a format reserve area (5 bytes), a dispersion information ECC area (2 bytes), and a data ECC area (3 bytes). The dispersion information ECC area contains redundant data for an error correction process against the management flag area, the logical address area, and the format reserve area. The data ECC area contains redundant data for an error correction process against 512-byte data.

Detail Description Paragraph:
[0104] In other words, a record command issued by the remote controller of the user or the like is supplied to the DSP 30 from the external controller through the bus and the bus interface 32. The encoder/decoder IC 10 compresses the received audio data and supplies the resultant ATRAC3 data to the security IC 20. The security IC 20 encrypts the ATRAC3 data. The encrypted ATRAC3 data is recorded to the flash memory 42 of the memory card 40. Thereafter, the FAT and the management file are updated. Whenever a file is updated (in reality, whenever the recording process of audio data is completed), the FAT and the management file stored in the SRAMs 31 and 36 are rewritten. When the memory card 40 is detached or the power of the recorder/player is turned off, the FAT and the management file that are finally supplied from the SRAMs 31 and 36 are recorded to the flash memory 42. Alternatively, whenever the recording process of audio data is completed, the FAT and the management file written in the flash memory 42 may be rewritten. When audio data is edited, the contents of the management file are updated.

Detail Description Paragraph:
[0501] FIG. 30 shows the data arrangement (for one block) of the ATRAC3 data file A3Dnnnn in the case that 1 SU is composed of N bytes. In this file, one slot is composed of eight bytes. FIG. 30 shows the values of the top portion (0x0000 to 0x3FF8) of each slot. The first four slots of the file are used for a header. As with the data block preceded by the attribute header of the data file (see FIG. 17) of the first example, a header is placed. The header contains an area BLKID-A3D (4 bytes), a maker code area MCode (2 bytes), an area BLOCK SEED (8 bytes) necessary for encrypting process, an area CONNUM0 (4 bytes) for the initial contents cumulation number, a serial number area BLOCK SERIAL (4 bytes) for each track, and an area INITIALIZATION VECTOR (8 bytes) necessary for encrypting/decrypting process. The second last slot of the block redundantly contains an area BLOCK SEED. The last slot contains areas BLKID-A3D and MCode. As with the first embodiment, the header is followed by the sound unit data SU-nnnn.

Detail Description Paragraph:
[0531] A forge-check code is generated by calculating CONTENTS KEY (CK) of an ATRAC3 data file generated along with the reproduction management file PBLIST.MSF using the hash function. In addition, since the file may be erased or moved, the value of CONTENTS KEY (CK) is stored in another file. When clock information S-YMDhms has not been entered, all hash values are set to zero with no calculations. Whenever the clock information S-YMDhms is updated, the hash values are calculated.

Detail Description Paragraph:
[0538] The match detecting circuit 74 compares the current hash values with the former hash values. Depending on whether the current hash values are the same as

the former hash values, it is determined whether the reproduction limitation value block 70 has been forged. Output data of the match detecting circuit 74 is supplied to the controlling portion 75.

Detail Description Paragraph:
[0542] The calculating process of this example is performed in the same manner as that for an ATRAC3 data file. The circuit of this calculating process can be shared with that for the ATRAC3 data file. Since the file may be erased or moved, the value of CONTENTS KEY (CK) is stored in another file. When clock information S-YMDhms has not been entered, all hash values are set to zero with no calculations. Whenever the clock information S-YMDhms is updated, the hash values are calculated.

Detail Description Paragraph:
[0546] At step SP103, with CONTENTS KEY (CK) contained in the attribute header, the hash calculating circuit 71 calculates the clock information S-YMDhms of the reproduction management file PBLIST.MSF using the hash function and stores the calculated value to the memory area 73 of the encrypting circuit 22.

Detail Description Paragraph:
[0555] The match detecting circuit 74 compares the currently calculated hash values with the formerly calculated hash values. When they match, it is determined that any information of track attribute A, reproduction limitation flag, security version LT, MG (D) serial number MG (D) Serial, contents cumulation number CONNUM, reproduction start date/time YMDhms-S, reproduction expiration date/time YMDhms-E, number of track reproduction times CT, number of reproduction permission times MT, COPY CONTROL CC, and number of high speed digital copy permission times CN (optional) of the attribute file has not been forged. Thereafter, the flow advances to step SP114. At step SP114, the reproducing operation of the ATRAC3 data file is permitted.

Detail Description Paragraph:
[0561] After the memory card 40 is detached and then attached again, when the reproduction command is issued at step S3, the flow advances to step S202. At step S4, the hash calculating circuit 71 calculates hash values of the reproduction limitation value block 70. The hash values calculated by the hash calculating circuit 71 are stored as current hash values to the memory area 72 of the encrypting circuit 22. The current hash values and the former hash values are read and supplied to the match detecting circuit 74. The match detecting circuit 74 compares the current hash values with the former hash values. Depending on whether they match, the match detecting circuit 74 determines whether or not the reproduction limitation value block 70 has been forged. The match detecting circuit 74 supplies the detected result to the controlling portion 75.

Detail Description Paragraph:
[0563] After the memory card 40 is detached and then attached again, when the reproduction command is issued at step S7, the flow advances to step S203. At step S203, the same process as step S202 is performed. In other words, hash values of the reproduction limitation value block 70 are calculated and compared with the former hash values. Thus, it is determined whether or not the reproduction limitation value block 70 has been forged (at step S8). When the reproduction limitation value block 70 has not been forged, the reproducing operation is performed (at step S9). Thereafter, the number of reproduction times CT is decremented by 1 and thereby (CT=0) is set (at step S10).

Detail Description Paragraph:
[0564] After the number of reproduction times CT is set to zero (CT=0), regardless of whether the reproduction limitation value block 70 has been forged, the number of reproduction times CT is considered with priority. Thus, the reproducing operation is prohibited. For example, after the memory card 40 is detached and then

attached again, when the reproduction command is issued at step S11, the flow advances to step S12. At step S12, hash values of the reproduction limitation value block 70 are calculated and then the current hash values are compared with the former hash values. Since the current hash values match the former hash values, normally, the reproducing operation is permitted. However, since the number of reproduction times CT is zero (CT=0), the reproducing operation is prohibited. Thus, in this case, the controlling portion 75 forms control information that prohibits the reproducing operation (at step S13). In addition, with a speaker and/or a display, the user is informed that because the number of reproduction times CT matches the number of reproduction permission times MT, the reproducing operation is prohibited.

Detail Description Paragraph:
[0571] After the memory card 40 is detached and then attached, when the reproduction command is issued, hash values of the reproduction limitation value block 70 are calculated. The match detecting circuit 74 compares the hash values currently calculated with the hash values formerly calculated. Depending on whether they match, the match detecting circuit 74 determines whether the reproduction limitation value block 70 has been forged. In addition, the match detecting circuit 74 compares the date/time of the inner clock 76 with the reproduction expiration date/time. When the reproduction limitation value block 70 has not been forged and the date/time of the inner clock 76 is before the reproduction expiration date/time as the determined results of the match detecting circuit 74, the reproducing operation is performed.

Detail Description Paragraph:
[0573] In other words, before a data file is reproduced, the current hash values and the former hash values are compared. When they do not match, since it is determined that the reproduction limitation value block 70 has been forged, the reproducing operation is prohibited. However, even if the current hash values match the former hash values, unless the reproduction expiration date/time is proper, the reproducing operation is prohibited. When the reproducing operation is prohibited, with the speaker or display, the user is informed of a relevant message. Even if the date/time of the inner clock 76 exceeds the reproduction expiration date/time, hash values of the reproduction limitation value block 70 are calculated and stored against future forged information.

Detail Description Paragraph:
[0576] For example, after the memory card 40 is detached and then attached, when the reproduction command is issued, the current hash values and the former hash values are compared. Corresponding to whether or not they match, it is determined whether or not the reproduction limitation value block 70 has been forged. In addition, the date/time of the inner clock 76 and the reproduction start date/time are compared. When the reproduction limitation value block 70 has not been forged and the date/time of the inner clock 76 exceeds the reproduction state date/time as the determined results, the reproducing operation is permitted.

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 6 of 6 returned.

☐ 1. Document ID: US 20030120604 A1

Using default format because multiple data bases are involved.

L14: Entry 1 of 6 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

US-CL-CURRENT: 705/57; 705/400, 705/50

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. D

☐ 2. Document ID: US 20020007452 A1

L14: Entry 2 of 6 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007452
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007452 A1

TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
TRAW, CHANDLER BRENDAN STANTON	PORTLAND	OR	US	
AUCSMITH, DAVID WAYNE	PORTLAND	OR	US	

US-CL-CURRENT: 713/152; 380/201, 705/57

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 3. Document ID: US 6859790 B1

L14: Entry 3 of 6 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 4. Document ID: US 6246767 B1

L14: Entry 4 of 6 File: USPT Jun 12, 2001

US-PAT-NO: 6246767
DOCUMENT-IDENTIFIER: US 6246767 B1
** See image for Certificate of Correction **

TITLE: Source authentication of download information in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 5. Document ID: US 6076077 A

L14: Entry 5 of 6 File: USPT Jun 13, 2000

US-PAT-NO: 6076077
DOCUMENT-IDENTIFIER: US 6076077 A
** See image for Certificate of Correction **

TITLE: Data management system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw D

☐ 6. Document ID: US 5666415 A

L14: Entry 6 of 6 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L13 and L10	6

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Day : Saturday
Date: 4/16/2005

PALM INTRANET

Time: 12:31:20

Content Information for 09/711747

Search Another: Application# [ ] Search **or Patent#** [ ] Search
PCT / [ ] / [ ] Search **or PG PUBS #** [ ] Search
Attorney Docket # [ ] Search
Bar Code # [ ] Search

Appln Info | **Contents** | Petition Info | Atty/Agent Info | Continuity Data | Foreign Data

Date	Status	Code	Description
04/11/2005		FWDX	DATE FORWARDED TO EXAMINER
04/08/2005	80	A.NE	AMENDMENT AFTER FINAL REJECTION
03/11/2005	61	MCTFR	MAIL FINAL REJECTION (PTOL - 326)
03/07/2005	60	CTFR	FINAL REJECTION
01/04/2005		FWDX	DATE FORWARDED TO EXAMINER
01/03/2005	71	A...	RESPONSE AFTER NON-FINAL ACTION
12/02/2004		DOCK	CASE DOCKETED TO EXAMINER IN GAU
10/01/2004	41	MCTNF	MAIL NON-FINAL REJECTION
09/28/2004	40	CTNF	NON-FINAL REJECTION
06/17/2004		TSSCOMP	IFW TSS PROCESSING BY TECH CENTER COMPLETI
06/17/2004		FWDX	DATE FORWARDED TO EXAMINER
05/21/2004	71	A...	RESPONSE AFTER NON-FINAL ACTION
05/21/2004		WAMD	WORKFLOW INCOMING AMENDMENT IFW
04/21/2004	41	MCTNF	MAIL NON-FINAL REJECTION
03/22/2004	40	CTNF	NON-FINAL REJECTION
03/18/2004		DOCK	CASE DOCKETED TO EXAMINER IN GAU
03/11/2004		DOCK	CASE DOCKETED TO EXAMINER IN GAU
04/23/2002		DOCK	CASE DOCKETED TO EXAMINER IN GAU
06/28/2001		M844	INFORMATION DISCLOSURE STATEMENT (IDS) FIL
05/19/2001	30	DOCK	CASE DOCKETED TO EXAMINER IN GAU
04/14/2001	20	OIPE	APPLICATION DISPATCHED FROM OIPE
04/14/2001		COMP	APPLICATION IS NOW COMPLETE
02/20/2001		INCD	NOTICE MAILED--APPLICATION INCOMPLETE--FILI
02/17/2001		C.AD	CORRESPONDENCE ADDRESS CHANGE
12/15/2000		SCAN	IFW SCAN & PACR AUTO SECURITY REVIEW
11/13/2000	19	IEXX	INITIAL EXAM TEAM NN

L14: Entry 4 of 6 File: USPT Jun 12, 2001

DOCUMENT-IDENTIFIER: US 6246767 B1
** See image for Certificate of Correction **
TITLE: Source authentication of download information in a conditional access system

Application Filing Date (1):
20000120

Detailed Description Text (19):
In FIG. 2A, clear services such as the elementary digital bit streams which comprise MPEG-2 programs are sent through a 1.sup.st level encryption called the Program Encrypt function 201, which is preferably a symmetric cipher such as the well-known DES algorithm. Each elementary stream may be individually encrypted and the resulting encrypted streams are sent to MUX 200 to be combined with other elementary streams and private data, such as conditional access data. The key used in the Program Encrypt function 201 is called the Control Word (CW) 202. The CW 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs. A new CW is generated frequently, perhaps once every few seconds and is applied to each elementary stream on the same time scale. Each new CW is encrypted by Control Word Encrypt & Message Authenticate function 204 using a Multi-Session key (MSK) 208 provided by Multi-Session Key generator 205. The CW is then combined into an ECM 107 with other service-related information. The ECM 107 is authenticated by Control Word Encrypt & Message Authenticate function 204 which produces a message authentication code using a keyed-hash value derived from the message content combined with a secret which can be shared with the receiving set-top box 113. This secret is preferably part or all of the MSK 208. The message authentication code is appended to the rest of the ECM 107. The CW 202 is always encrypted before being sent along with the other parts of the ECM to MUX 200. This encryption is preferably a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208).

Detailed Description Text (30):
Once the sealed digest is made, the contents of the EMM (here, MSK 309 and the related information) are encrypted with the public key DHCT Ku 312 of the DHCT 333 to which EMM 315 is addressed and EMM 315, containing the encrypted contents and the sealed digest, is sent via transmission medium 331 to the DHCT 333. In the following, the notation Kr is used to indicate a private key and Ku is used to indicate a public key. The notation RSA indicates that the encryption is done using the well-known RSA public key encryption algorithm.

Detailed Description Text (33):
ECM 323 is sent together with encrypted content 329 to DHCT 333. The first ECM 323 for a given portion of encrypted content 329 must of course arrive at DHCT 333 before the encrypted content does. In the preferred embodiment, content 325 and ECM 323 are encoded according to the MPEG-2 standard. The standard provides for a transport stream which includes a number of component streams. Some of these carry content 329, another carries the ECMs 323, and a third carries the EMMs 315. Only the streams carrying content 329 are encrypted according to DES 329; since the control words in ECMs 323 and the contents of EMMs 315 have already been encrypted,

no further encryption is needed when they are sent in the MPEG-2 transport stream. The manner in which EMMs and ECMs are transported in the MPEG-2 transport stream will be described in more detail later.

Detailed Description Text (34):
When an ECM 323 is received in DHCT 333, control word 319 is either decrypted or found by encrypting the counter value at 343 using the MSK. The integrity of the contents of the ECM 323 is checked by comparing the value resulting from hashing the contents plus some or all of the MSK (based on cryptographic principles) in the one-way hash function with the message digest contained in ECM 323. Included in the contents are control word 319 and information identifying the service instance 325 which ECM 323 accompanies. The identifying information is used together with the authorization information received with EMM 315 to determine whether DHCT 333 is authorized to receive the service instance 325. If it is, control word 319 is used in service decryptor 347 to decrypt encrypted content to produce original content 325.

Detailed Description Text (35):
System 301 offers a number of advantages with regard to security. It takes advantage of the speed of symmetrical encryption systems where that is needed to decrypt encrypted content 329 and the control word in ECM 323. The control word is protected by encrypting it using the MSK, and ECM 323 is authenticated by using some or all of MSK 309 as a shared secret between the entitlement agent and DHCT 333. MSK 309 is protected in turn by the fact that it is sent in an EMM which is encrypted using the DHCT's public key and by the fact that the EMM includes a sealed digest which is encrypted using the entitlement agent's private key. Further security is provided by the fact that service identification information from ECM 323 must agree with the authorization information received in EMM 315 before control word 319 is provided to service decryptor 347. For example, as described in detail in the Banker and Akins parent patent application supra, one use of the information in ECM 323 and EMM 315 is to prevent what are termed "replay attacks" on the encrypted services. In addition to being secure, system 301 is flexible. The authorization information contained in EMM 315 and the service identification information contained in ECM 323 together permit a wide range of access to service instances received in DHCT 333.

Detailed Description Text (59):
At the entitlement agent, key 420 is decrypted using the entitlement agent's private key 310, and the sealed digest is decrypted using the public key 312 of the DHCT. If the Encrypted Forwarded Entitlement Information (EFEI) 419 contained in the FPM 421 is determined not to have been tampered with, it is passed to 3DES decryption 443, which decrypts it using key 420 and provides forwarded entitlement information 417 to the entitlement agent. As will be immediately apparent, the same technique, with or without the 3DES encryption of the contents of the message, can be used to send messages to any entity for which DHCT 333 has the public key. At a minimum, this includes the CAA and any entitlement agent which has been allocated memory in DHCT 333.

Detailed Description Text (70):
1. encrypting the service content

Detailed Description Text (90):
Service Encryption and ECM Streamer (SEES) module 620 is a component of QAM Modulator 619 that operates under direction of control suite 607 to encrypt the MPEG-2 transport stream packets that are employed in the preferred embodiment to transmit service content 325. As shown in FIG. 6, service content 325 may be received from sources such as a digital satellite distribution system 613, a digital terrestrial distribution system 611, or a media server 609. Media server 609 may be connected to head end 515 by a broadband integrated gateway 615. SEES 620 uses MSK 309 to generate the control words 319 used for service encryption and

creates ECMs 323 for transporting the control words together with encrypted service content 329 within the outgoing MPED-2 Transport Stream. SEES 620 encrypts the control words in the ECMs 323 with MSKs 309. The MSKs are generated by TED 603 and are sent to SEES 620 in encrypted form in EMM-like messages.

Detailed Description Text (124):
an identifier for the type of security algorithm used with the message, including encryption of the message and authentication of its contents; and

Detailed Description Text (213):
Of the non-event broadcast EMMs, four types will be discussed here. These are Update MSK, Update Bit Map, Update List, and update combinations with MSK and list or bitmap. Those skilled in the art will be able to easily apply the principles explained below to EMMs that perform the functions indicated by the names of the other non-event broadcast EMMs. For example, the principles of digital EMMs can be applied to analog EMMs. There is a separate type of NVSC 1405 for each information type provided by the above non-event broadcast EMMs. FIG. 16 shows the contents of four of these types of NVSCs. Each NVSC type will be discussed together with the EMM that provides the information it contains.

Detailed Description Text (245):
DHCT 333 sends a forwarded purchase message with the purchase information via the reverse channel to the entitlement agent that sent the GBAM. The FPM is contained in a reverse channel data packet that is addressed to the EA. FIG. 21 provides an overview of the FPM and of the cryptographic measures used to protect its contents. FPM 2101 is a CA message 805 and consequently is sent with a CA message header 1003. FPM 2101 itself is made up of FPM encrypted envelope key 2103, which contains the EAID for the entitlement agent and FPM key 2119 for decrypting the purchasing information contained in FPM encrypted events 2113. The key and other contents of envelope key 2103 are encrypted for privacy using the public key of the entitlement agent for which FPM 2101 is intended. CA FPM message 2105 includes CA FPM header 211, which includes the EAID for the intended EA, and FPM encrypted events 2113. The latter are encrypted using the 3-DES algorithm with the key in envelope key 2103. CA FPM message 2105's parts are a header 213, FPM clear events 2133, which contains the purchase information, and padding 2135. The last part of FPM 2101 is FPM signed authentication 2107, which is encrypted with the private key of DHCT 333 from which FPM message 2101 is sent. The encrypted material includes FPM signing header 2125, FPM MAC 2127, and padding 2129. FPM MAC 2127 is made using the MD 5 one-way hash algorithm from FPM clear events 2133. Only the EA for which the FPM is intended can decrypt envelope key 2103 to obtain key 2119 to decrypt FPM encrypted events 2123, and the EA can check the authenticity of FPM clear events 2133 only if it has the public key for DHCT 333 from which FPM 2101 was sent.

Detailed Description Text (333):
(4) uses the decrypted encrypted events with MD5 code 2529 to produce a new hash which it compares with the decrypted value of FPM authentication 2107. If this comparison indicates that the FPM is authentic, TED 2425(i) returns the decrypted events to DNCS 507, which in turn forwards them to EA 2409(i).

Detailed Description Text (334):
The MSKs in MSK 2515 are generated by TED 2425(i). The interface for MSK generation simply requires the MSKID for the new MSK, the parity for the new MSK, and any expiration time. MSK generation code 2525 receives a random number from random number generator 2537 and uses it to generate the new MSK. Then the MSKE 2515 for the new MSK is made and added to EA information 2507. If there is already an MSKE 2525 for the MSKID for the new MSK, the new MSKE replaces the existing MSKE. TED 2425(i) also generates interactive session keys for the add interactive session EMM. Key generation is as described for the MSK EMM. Once TED 2425(i) has provided the EMM content with the encrypted key to DNCS 507, it overwrites the area in memory 2505 where the interactive session key was stored.

Detailed Description Text (343):
Code message 2301 can be sent either in a MPEG-2 transport stream or as an IP packet. Message 2301 may be broadcast to any DHCT 333 that has the authenticating CAA or EA, or it may be sent to a specific DHCT 333. In that case, the packet(s) carrying code message 2301 will include an address for DHCT 333. In the preferred embodiment, the address is DHCT 333's serial number. When code message 2301 arrives in the DHCT 333 for which it is intended, code executing on the processor performs the one-way hash function on code 2305 and provides the result together with AID 2307 and sealed digest 2309 to DHCTSE 627. DHCTSE 627 uses AID 2307 to locate the public key for the CAA or EA and then uses the public key to decrypt sealed digest 2309. Finally, it compares the hash value in decrypted sealed digest 2309 with that provided by the code executing on the processor, and, if they are equal, DHCTSE 627 signals that the code has been authenticated.

Current US Cross Reference Classification (4):
380/30

Previous Doc Next Doc Go to Doc#

L14: Entry 5 of 6 File: USPT Jun 13, 2000

DOCUMENT-IDENTIFIER: US 6076077 A
** See image for Certificate of Correction **
TITLE: Data management system

Abstract Text (1):
A system for dealing in an original data content and an edited data content. A data content is handled as an object, and the data content is edited by editing a data content, functioning as an object, in accordance with an edit program. The edited data content is expressed by the original data content and the editing scenario which describes editing detail by the edit program. Only the encrypted editing scenario is dealt in. Upon receipt of the encrypted editing scenario, a user decrypts the encrypted editing scenario using a crypt key obtained from a key management center, and obtains the original data content from the database in accordance with the editing scenario and re-constitutes the edited data content. In case there is the one who wishes sale of the editing scenario, its utilization right is sold by auction.

Application Filing Date (1):
19970501

Brief Summary Text (11):
The database copyright management system of the above application in order to manage the copyright, either one or more of a program for managing the copyright, copyright information, and a copyright control message are used in addition to a use permit key corresponding to a requested use, and data content which has been transferred with encryption is decrypted to be used for viewing and editing, and the data content is encrypted again when used for storing, copying and transferring.

Brief Summary Text (14):
The above-mentioned system comprises a key management center that manages a crypt key and a copyright management center that manages the database copyright. According to this system, all of the data content delivered from a database is encrypted by a first crypt key, and a first user who wishes to uses data content directly from the database requests the key management center the key corresponding to the specific usage by presenting information on the first user to the center. In response to the primary usage request from the first user, the key management center transfers the information on the first user to the copyright management center. On receiving the information, the copyright management center transfers this information together with a copyright management program to the key control center. On receiving the copyright management program, the key control center transfers the first crypt key and a second crypt key K2 corresponding to the specific usage together with the copyright management program to the first user via a communication network. On receiving the first crypt key, the first user uses this key to decrypt the data content for usage. The user uses the second crypt key to encrypt and decrypt data content when subsequently storing, copying or transmitting the data content.

Brief Summary Text (40):
Here, the operation to encrypt data content, a plain text material M to a

cryptogram Cmks using a secret-key Ks is expressed as:

Brief Summary Text (42):
Also, the operation to encrypt the plain text data content M to a cryptogram Cmkb using a public key Kb is expressed as:

Brief Summary Text (44):
The operation to encrypt the plain text data content M to a cryptogram Cmkv using a private-key Kv is expressed as:

Brief Summary Text (46):
The encryption technique is the means to exclude illegitimate use of data content, but perfect operation is not guaranteed. Thus, the possibility of illegitimate use of data content cannot be completely excluded.

Brief Summary Text (50):
In the present application, a data content is handled as an object, and the data content, functioning as an object, is edited in accordance with a edit program. Therefore, the edited data content can be expressed by the original data content and the editing scenario, which describes the edit detail based on an edit program. As the original data content to be utilized, there are, in addition to the one stored in the database, those prepared originally by the data editor. The data content prepared by the data editor can also be handled in the same manner as the other data by storing it in the database. In this case, only the encrypted editing scenario is dealt in, and when the user obtains the encrypted editing scenario, the user decrypts the encrypted editing scenario by using a crypt key obtained from a key management center, and obtains the original data content from the database in accordance with the editing scenario and reconstitutes the edited data content.

Detailed Description Text (15):
The databases 1, 2, and 3, copyright management center 8, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-th user terminal 7 are connected to communication line 9. In FIG. 1, encrypted data content is transmitted via the path shown by a broken line, requests are transmitted from user terminal 4, 5, 6, or 7 to database 1, 2, or 3 and copyright management center 8 via the path shown by a solid line. The permit key, copyright management program, and crypt key corresponding to a specific usage are transmitted from database 1, 2, or 3 and copyright management center 8 to user terminal 4, 5, 6, or 7 via the path shown by an one-dot chain line.

Detailed Description Text (16):
The Embodiment 1 employs a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2 that are prepared by a first user, and a first secret-key Ks1 and a second secret-key Ks2 prepared by the database. The database uses the first secret-key Ks1 to encrypt data content M:

Detailed Description Text (19):
The database then transmits these encrypted data content Cmks1 and the first and the second secret-keys Cks1kb1 and Ck2kb2 to the first user.

Detailed Description Text (21):
and decrypts the encrypted data content Cmks1 by the decrypted first secret-key Ks1:

Detailed Description Text (23):
which is subsequently used as a key for encrypting/decrypting of storing, copying, or transmitting data content.

Detailed Description Text (27):

Databases 1, 2, and 3 store text data content or binary, digital audio, or digital picture data content constituting computer graphics screens or programs in unencrypted form. This data content is encrypted and supplied to the user terminal 4 via communication line 8 during a data content read operation in response to a request from first user terminal 4.

Detailed Description Text (31):
The original data content M1, M2 and M3 are encrypted using each of the second secret-keys Ks21, Ks22, Ks23 supplied with each of data content M1, M2 and M3 when used for operations other than display; i.e., store, edit, copy or transmit:

Detailed Description Text (32):
The data content parts M4, M5 and M6, of original data content are also encrypted using each of the second secret-keys Ks21, Ks22, Ks23 supplied with each of the original data content when used for operations other than display:

Detailed Description Text (34):
and supplies encrypted original data content parts Cm4ks21, Cm5ks22 and Cm6ks23 to second user together with the edit program Pe with the digital signature, via communication line 9 or by storing into the recording medium 10.

Detailed Description Text (35):
Upon receipt of the encrypted original data content parts Cm4ks21, Cm5ks22 and Cm6ks23, and the edit program Pe, second user requests second secret-keys Ks21, Ks22, Ks23 for decryption of the encrypted original data content parts Cm4ks21, Cm5ks22 and Cm6ks23 by presenting the edit program Pe with the digital signature, to the copyright management center 8.

Detailed Description Text (42):
By incorporating the agent program into a basic system of a data copyright management system so that the database utilization of a user is monitored, and it is arranged that information including data utilization condition and charging is collected at the database or the copyright management center, using metering function placed in user terminal, and thus, it is possible to know the database utilization condition of the user at the database side or the copyright management center side and achieve more accurate copyright management. These agent program and its data are also necessary to be protected in copyrights, and therefore, are encrypted like original data content.

Detailed Description Text (48):
The solid line, broken line and one-dot chain line in this FIG. 3 show the path for data content and requests for crypt keys, path of encrypted data content and path of crypt keys, respectively.

Detailed Description Text (50):
In the data copyrights management system, the original data content provided by each of information providers 15 and 16 has been encrypted to protect the copyright. Therefore, the use of the encrypted original data content obtained by first user 13 needs to be decrypted. All of the crypt keys for the decryption are deposited in key control center 12 to be controlled by the center.

Detailed Description Text (52):
In this system, plaintext original data content M0 is encrypted by first secret-key Ks1:

Detailed Description Text (54):
Original plaintext copyright label Lc0 is attached to encrypted original data content Cm0ks1 provided for primary users 13, and is used for obtaining primary use permit keys, etc. Namely, encrypted original data content Cm0ks1 includes plaintext original copyright label Lc0 and encrypted original data content Cm0ks1. The name

of application programs in use, outlined explanation, fees and charging method are entered into plaintext original copyright label Lc0 in addition to general information including the name of original creator, title name and creation date. The number of a crypt key is also entered if necessary. Digital signature by original creator added to plaintext original copyright label Lc0 prevents false copyright claiming.

Detailed Description Text (55):
Primary users 13 who require use of encrypted original data content Cm0ks1 make a request to key control center 12 via communication line 14 for distributing primary use permit keys K1 indicating original copyright label Lc0.

Detailed Description Text (58):
Primary users 13 decrypt encrypted primary copyrighted data content Cm0ks1 using first secret-key Ks1:

Detailed Description Text (60):
When decrypted original data content M0 is stored in primary users 13 devices, it is encrypted again by first secret-key Ks1

Detailed Description Text (61):
and re-encrypted original data content Cm0ks1 is stored.

Detailed Description Text (62):
For repeated use of re-encrypted original data content Cm0ks1, repeated decryption and encryption are carried out using first secret-key Ks1.

Detailed Description Text (64):
When halfway edited data content M0' is stored in users 13 devices, it is encrypted by second secret-key Ks2:

Detailed Description Text (66):
When primary users 13 copy editorial data content M1 into external recording medium 18 or transfer it via communication line 14, they encrypt editorial data content using third secret-key Ks3:

Detailed Description Text (68):
Secondary users 19 who desire to use provided encrypted editorial data content Cm1ks3 request key control center 12 for distributing third secret-key Ks3 via communication line 14. Key control center 12 that has received the request for distributing third secret-keys Ks3 from secondary users 19 distributes third secret-key Ks3 to secondary users 19 via communication line 14.

Detailed Description Text (69):
Secondary users 19 who have received third secret-keys Ks3 decrypt encrypted editorial data content Cm1ks3 using third secret-key Ks3:

Detailed Description Text (71):
When using encrypted data content Cm1ks3 again, decryption and encryption are carried out using third secret-key Ks3 also in this case.

Detailed Description Text (76):
It is also possible that the original author A stores the original secret-key Ks0 and encrypts the original data content M0 without depending on the data management center, while the original secret-key Ks0 must be stored at the data management center to utilize the original data content M0 by the user (data content user).

Detailed Description Text (81):
encrypts the original data content M0 using the decrypted original secret-key Ks0:

Detailed Description Text (82):
and transfers the encrypted original data content Cm0ks0, the original copyright label Lc0 and the original copyright label fingerprint F0 to the first user U1.

Detailed Description Text (83):
(4) When the encrypted original data content Cm0ks0, the original copyright label Lc0 and the original copyright label fingerprint F0 are transferred, the first user U1 presents the original copyright label Lc0, the original copyright label fingerprint F0 and first user label Lu1 and requests the data management center to distribute the original secret-key Ks0.

Detailed Description Text (87):
decrypts the encrypted original data content Cm0ks0 using the decrypted original secret-key Ks0:

Detailed Description Text (90):
The copyright of the original author relating to the original data content M0 can be protected by the original copyright label Lc0 which has been registered, original copyright label fingerprint F0 and the original secret-key Ks0 corresponding to the original copyright label Lc0 and also by the first user label Lu1 and the first secret-key Ks1 corresponding to the first user label Lu1. However, because no key for encrypting the edited data content Me1 is available, the secondary copyright of the first user relating to the edited data content Me1 is not yet protected.

Detailed Description Text (97):
encrypts the first edited data content Me1 using the decrypted first edit secret-key Kse1:

Detailed Description Text (98):
and transfers the encrypted first edited data content Cme1kse1 to the second user U2 together with the first edit label Le1, and the electronic fingerprint Fe1 of the first edit label Le1.

Detailed Description Text (100):
Each user may put digital signature which one-way hash value of the user's label is encrypted using user's private-key on the user's label to be presented to the data management center. Then, the data management center decrypts the encrypted one-way hash value using the user's public-key, calculates the one-way hash value of the label and compares the two one-way hash values in order to verify validity of each user's label.

Detailed Description Text (101):
In this embodiment, only the first edit label Le1 and the electronic fingerprint Fe1 of the first edit label Le1 are transferred together with the encrypted first edited data content Cme1kse1 when edited data content transfer, while it is possible to arrange in such manner that the other labels and electronic fingerprints can be simultaneously transferred.

Detailed Description Text (103):
In the systems described above, the data content is encrypted using secret-key, and the secret-key for its decryption and secret-key for re-encryption used for storage, copying and transfer are distributed by the data management center based on the user label presented by the user.

Detailed Description Text (109):
To protect data content copyright, it is necessary to use some sort of encryption technique to restrict unauthorized utilization of the data content.

Detailed Description Text (110):

In the Embodiment 3 described above, to protect copyright in a system for an ordinary computer having data storage unit, encrypted data content and labels not encrypted as clues to utilize the data content are used.

Detailed Description Text (111):
In contrast, in a system for a network computer, which has only the function of the above-mentioned terminal unit, the data content is not stored, copied or transferred, and there is no need to encrypt the data content.

Detailed Description Text (116):
In the system of this embodiment, public-key and private-key are used. If original data content is transferred to a user, the original data content is encrypted by using a secret-key or a public-key of transferred destination for the purpose of security.

Detailed Description Text (121):
(1)(2) The first user U1 presents the first user label Lu1 to the data management center, collects the original data content M0i (i=1, 2, 3, . . .) from data content library of the information provider IP in the system and obtains a edit tool Pe. In this case, the original data content M0i and the edit tool Pe are encrypted using public-key Kb1 of the first user U1:

Detailed Description Text (122):
and the encrypted original data content Cm0ikb1 and the encrypted edit tool Cpekb1 are distributed to the first user U1.

Detailed Description Text (124):
(3) When the encrypted original data content Cm0ikb1 and the encrypted edit tool Cpekb1 are distributed, the first user U1 decrypts the distributed encrypted original data content Cm0ikb1 and the encrypted edit tool Cpekb1 using private-key Kv1 of the first user U1:

Detailed Description Text (126):
(4) Obtaining the first edited data content M1i, the first user U1 encrypts a first scenario S1i, which is the editing process data content for the first edited data content M1i, using public-key Kbc of the data management center:

Detailed Description Text (133):
and transfers the encrypted first edit label Cle1kb2 to the second user U2, but the first edited data content M1i or the encrypted first edited data content is not transferred to the second user U2.

Detailed Description Text (141):
When the first edited data content M1i is reproduced, the data management center encrypts the first edited data content M1i and the edit tool Pe using the public-key Kb2 of the second user U2:

Detailed Description Text (142):
and transfers the encrypted first edited data content Cm1ikb2 and the encrypted edit tool Cpekb2 to the second user U2.

Detailed Description Text (143):
(9) When the encrypted first edited data content Cm1ikb2 and the encrypted edit tool Cpekb2 are distributed, the second user U2 decrypts the distributed encrypted first edited data content Cm1ikb2 and the encrypted edit tool Cpekb2 using private-key Kv2 of the second user U2:

Detailed Description Text (145):
(10) When the second edited data content M2i is obtained, the second user U2 encrypts the second scenario S2i, which is editing process data content of the

second edited data content M2i, using the public-key Kbc of the data management center:

Detailed Description Text (149):
prepares a second edit label Le2 based on the presented user label of the second user and the decrypted second scenario S2i, stores it in the data content management center, encrypts the second edit label Le2 using public-key Kb2 of the second user U2:

Detailed Description Text (163):
The key management center stores a secret key for encryption/decryption for the original data content, the user data content and the editing scenario and supplies it in response to the request of the user.

Detailed Description Text (167):
(1) The information provider IPi (i=1, 2, 3, . . . ; the same applies hereinafter) encrypts the original data content M0i using an original secret-key K0i:

Detailed Description Text (168):
encrypts the corresponding original secret-key Ks0i using a public key Kbc of the data content dealing center:

Detailed Description Text (169):
and supplies the encrypted original data content Cm0iks0i (shown as "m0i" in the figure) and the encrypted original secret-key Cks0ikbc (shown as "ks0i" in the figure) to the data content dealing center.

Detailed Description Text (172):
and the decrypted original secret-key Ks0i is used for encryption of the original data content M0i.

Detailed Description Text (173):
The data content dealing center decrypts the supplied encrypted original secret-key Cks0ikbc using a private-key Kvc of the data content dealing center:

Detailed Description Text (174):
decrypts the encrypted original data content Cm0iks0i using the decrypted original secret-key Ks0i:

Detailed Description Text (179):
(3) Upon receipt of the request for use of the original data content M0i, the data content dealing center confirms the user label Lu1i to check for fee charging and identification, and then, encrypts the original data content M0i using the corresponding original secret-key Ks0i:

Detailed Description Text (181):
and distributes the encrypte original data content Cm0iks0i and the encrypted original secret-key Cks0ikb1i to the first user U1i, and also charges for the original data content utilization to the first user U1i.

Detailed Description Text (182):
(4) When the encrypted original data content Cm0iks0i and the encrypted original secret-key Cks0ikb1i have been distributed, the first user U1i decrypts the encrypted original secret-key Cks0ikb1i using a private-key Kv1i of the first user U1i:

Detailed Description Text (183):
decrypts the encrypted original data content Cm0iks0i using the decrypted original secret-key Ks0i:

Detailed Description Text (190):
For this purpose, the first user U1i prepares a first secret-key Ks1i, encrypts the first editing scenario S1i and the first user data content Mu1i using the first secret-key Ks1i:

Detailed Description Text (191):
encrypts the first secret-key Ks1i using a public-key Kbc of the data content dealing center:

Detailed Description Text (192):
and transfers the encrypted first editing scenario Cs1iks1i (shown as "s1i" in the figure), the encrypted first user data content Cmu1iks1i (shown as "m1i" in the figure), and the encrypted first secret-key Cks1ikbc (shown as "ks1i" in the figure) to the data content dealing center.

Detailed Description Text (195):
and the decrypted first secret-key K1i is used to encrypt the first editing scenario S1i and the first user data content Mu1i.

Detailed Description Text (196):
The data content dealing center decrypts the transferred encrypted first secret-key Cks1ikbc using a private-key Kvc of the data content dealing center:

Detailed Description Text (197):
decrypts the encrypted first editing scenario Cs1iks1i and the encrypted first user data content Cmu1iks1i using the decrypted first secret-key Ks1i:

Detailed Description Text (203):
(7) Upon receipt of the request for use of the original data content M0i and/or the first edited data content M1i, the data content dealing center confirms the user label Lu2i to check for fee charging and identification. Then, the original data content M0i requested for use, is encrypted using the corresponding original secret-key Ks0i. The first editing scenario S1i and the first user data content Mu1i are encrypted using the first secret-key Ks1i, the original secret-key Ks0i is encrypted using a public-key Kb2i, and the first secret-key Ks1i is encrypted using the public-key Kb2i:

Detailed Description Text (204):
Then, the encrypted original data content Cm0iks0i (shown as "m0i" in the figure), the encrypted first editing scenario Cs1iks1i (shown as "s1i" in the figure), the encrypted first user data content Cmu1iks1i (shown as "mu1i" in the figure), the encrypted original secret-key Cks0ikb2i and the encrypted first secret-key Cks1ikb2i are transferred to the second user U2i. And then, the data content dealing center charges for utilization of the original data content M0i and the first editing scenario S1i to the second user U2i.

Detailed Description Text (205):
(8) When the encrypted original data content Cm0iks0i, the encrypted first editing scenario Cs1iks1i, the encrypted first user data content Cmu1iks1i, the encrypted original secret-key Cks01kb2i and the encrypted first secret-key Cks1ikb2i have been transferred, the second user U2i decrypts the encrypted original secret-key Cks0ikb2i and the encrypted first secret-key Cks1ikb2i using a private-key Kv2i of the second user U2i :

Detailed Description Text (206):
Next, the encrypted original data content Cm0iks0i is decrypted using the decrypted original secret-key Ks0i, and the encrypted first editing scenario Cs1iks1i and the encrypted first user data content Cmu1iks1i are decrypted using the decrypted first secret-key Ks1i:

Detailed Description Text (209):
The second user U2i prepares a second secret-key Ks2i and encrypts a new second editing scenario S2i and a second user data content Mu2i, not stored in the database of the data content dealing center, using the second secret-key Ks2i:

Detailed Description Text (210):
Then, the second secret-key Ks2i is encrypted using the public-key Kbc of the data content dealing center:

Detailed Description Text (211):
and the encrypted second editing scenario Cs2iks2i (shown as "s2i" in the figure), the encrypted second user data content Cmu2iks2i (shown as "mu2i" in the figure), and the encrypted second secret-key Cks2ikbc (shown as "ks2i" in the figure) are transferred to the data content dealing center

Detailed Description Text (219):
The key management center stores a secret-key for encryption/decryption for the original data content, the editor's data content and the editing scenario and supplies it to the data content editor or the editing scenario seller.

Detailed Description Text (223):
(1) The information provider IPi (i=1, 2, 3, . . . ; the same applies hereinafter) encrypts the original data content M0i using an original secret-key K0i:

Detailed Description Text (224):
encrypts the corresponding original secret-key Ks0i using a public-key Kbc of the data content dealing center:

Detailed Description Text (225):
and supplies the encrypted original data content Cm0iks0i (shown as "m0i" in the figure) and the encrypted original secret-key Cks0ikbc (shown as "ks0i" in the figure) to the data content dealing center.

Detailed Description Text (228):
and the decrypted original secret-key Ks0i is used for encryption of the original data content M0i.

Detailed Description Text (229):
The data content dealing center decrypts the supplied encrypted original secret-key Cks0ikbc using a private-key Kvc of the data content dealing center:

Detailed Description Text (230):
decrypts the encrypted original data content Cm0iks0i using the decrypted original secret-key Ks0i:

Detailed Description Text (235):
(3) Upon receipt of the request for utilization of the original data content M0i, the data content dealing center confirms the user label Lei to check for fee charging and identification. Then, the original data content M0i is encrypted using the corresponding original secret-key Ks0i:

Detailed Description Text (236):
encrypts the original secret-key Ks0i using a public-key Kbei of the data content editor Ei:

Detailed Description Text (237):
and distributes the encrypted original data content Cm0iks0i and the encrypted original secret-key Cks0ikbei to the data content editor Ei, and further, charges a fee for the original data content utilization to the data content editor Ei and an end user.

Detailed Description Text (238):
(4) When the encrypted original data content Cm0iks0i and the encrypted original secret-key Cks0ikbei have been distributed, the data content editor Ei decrypts the encrypted original secret-key Cks0ikbei using a private-key Kvei of the data content editor Ei:

Detailed Description Text (239):
decrypts the encrypted original data content Cm0iks0i using the decrypted original secret-key Ks0i:

Detailed Description Text (246):
To sell the utilization right of the editing scenario S1i and the editor's data content Medi, the data content editor Ei prepares a secret-key Ksei, encrypts the editing scenario Sei and the editor's data content Medi using the secret-key Ksei:

Detailed Description Text (247):
and encrypts the secret-key Ksei using the public-key Kbc of the data content dealing center:

Detailed Description Text (248):
Then, the encrypted editing scenario Cseiksei (shown as "sei" in the figure), the encrypted editor's data content Cmeiksei (shown as "mei" in the figure), and the encrypted secret-key Ckseikbc (shown as "ksei" in the figure) are transferred to the data content dealing center.

Detailed Description Text (249):
The secret-key Ksei may be prepared by the data content editor Ei, or the data content editor Ei may ask the key management center to generate it. In case the key management center generates the secret-key Ksei, the generated secret-key Ksei is encrypted using the public-key Kbei of the data content editor Ei:

Detailed Description Text (250):
and the encrypted secret-key Ckseikbei is distributed to the data content editor Ei. The data content editor Ei decrypts it using own private-key Kvei:

Detailed Description Text (251):
and the decrypted secret-key Ksei is used to encrypt the editing scenario Sei and the data content editor's data content Medi.

Detailed Description Text (252):
The data content dealing center decrypts the transferred encrypted secret-key Ckseikbc using the private-key Kvc of the data content dealing center:

Detailed Description Text (253):
Then, the encrypted editing scenario Cseiksei and the encrypted editor's data content Cmediksei are decrypted using the decrypted secret-key Ksei:

Detailed Description Text (261):
The editing scenario seller Di, to whom it has been decided to sell, encrypts the secret-key Ksdi of the editing scenario seller Di using the public-key Kbc of the data content dealing center:

Detailed Description Text (263):
(8) The editing scenario market management center decrypts the presented encrypted secret-key Cksdikbc using the private-key Kvc of the data content dealing center:

Detailed Description Text (264):
encrypts the editing scenario Sei and the editor's data content Medi using the decrypted secret-key Ksdi of the editing scenario seller Di:

Detailed Description Text (265):
and sends the encrypted editing scenario Cseiksdi and encrypted editor's data content Cmediksdi to the editing scenario seller Di.

Detailed Description Text (270):
To cope with such problems, adopting a copyright management program and re-encryption of the data content is effective as the present inventor has proposed in the U.S. patent application Ser. No. 08/416,037 (EP 677949A2), and if adopting an arrangement referred to as a real-time OS or an embedded system which allows the copyright management program performing re-encryption to precede other application programs, the illegitimate use problems can be effectively avoided.

Current US Cross Reference Classification (1):
380/201

Current US Cross Reference Classification (5):
705/54

Current US Cross Reference Classification (6):
705/57

Current US Cross Reference Classification (9):
713/193

CLAIMS:

1. A method for dealing in data content using a data content dealing system, in which an original data content and an edited data content which a first user has edited are sold in a network to a second user, whereby:

said original data content comprises a data object;

said edited data content comprises said data object and an editing scenario describing editing details of said data object;

said data content dealing system comprises a data content dealing center and a database;

said data content dealing center comprises a key management center, a data content dealing management center and an editing scenario dealing management center; said method comprising the steps of:

said key management center generating a secret-key, storing said secret-key and transferring of said secret-key;

said data content dealing management center advertising and selling said data content stored in said database;

said editing scenario dealing management center advertising and selling said editing scenario;

said first user creating said edited data content by utilizing said original data content stored in said database, encrypting an editing scenario of said edited data content by a secret-key which is to be deposited in said database, and depositing said secret-key to said key management center;

transferring said encrypted editing scenario and said secret-key to the second user who wishes to utilize said edited data content;

said second user decrypting said encrypted editing scenario by said secret-key and re-constituting said edited data content according to said decrypted editing scenario.

3. The method of claim 1, wherein said step of transferring said encrypted editing scenario and said secret key to said second user comprises transferring said original data content to said second user together with said encrypted editing scenario and said secret-key.

4. A method of dealing in data content using a data content dealing system, in which a utilization right of an editing scenario of an edited data content which comprises an original data content edited by a data content editor is auctioned in a network to an editing scenario seller, whereby:

said original data content comprises a data object;

said edited data content comprises said data object and the editing scenario describing editing details of said data object;

said data content dealing system comprises a data content dealing center and a database;

said data content dealing center comprises a key management center, a data content dealing management center and an editing scenario market management center; said method comprising the steps of:

said key management center generating a secret-key, storing said secret-key and transferring said secret-key;

said data content dealing management center advertising and selling said original data content stored in said database;

said editing scenario market management center advertising and auctioning said editing scenario;

said data content editor producing the edited data content by utilizing said original data content stored in said database, encrypting the editing scenario of said edited data content by a secret-key of said data content editor, depositing said encrypted editing scenario of said edited data contend to said database and depcsiting said secret-key with said key management center;

auctioning said utilization right of said editing scenario to said editing scenario seller who wishes to sell said utilization right of said editing scenario;

said editing scenario seller transferring a secret-key for said editing scenario to said key management center;

said editing scenario market management center changing said secret-key for said editing scenario from the secret-key of said data content editor to the secret-key of said editing scenario seller.

Previous Doc Next Doc Go to Doc#

L14: Entry 6 of 6 File: USPT Sep 9, 1997

DOCUMENT-IDENTIFIER: US 5666415 A
TITLE: Method and apparatus for cryptographic authentication

Application Filing Date (1):
19950728

Detailed Description Text (5):
Server node 11 receives the secret sent by USER.sub.-- 1 10 and using the contents of table 15a in conjunction with the hashing functions 15b and encryption/decryption algorithms 15c, server node 11 determines whether USER.sub.-- 1 10 is an authorized user.

Detailed Description Text (21):
The first argument, which is a hash of a password using a third hashing function, provides protection against the server's database being compromised because an intruder accessing the contents of the database would be unable to determine the first argument which is to be provided by an authorized user. The database contains a second hash of the first argument, using a second hashing function. As hashes are one-way encryption algorithms, an intruder to the database would be unable to reverse the hash of the contents of the database, and as such would be unable to provide the proper first argument to the server. To check the validity of the first argument, the server applies a second hashing function to the first argument and compares the result to the server's database contents.

Detailed Description Text (23):
The second argument provided by the user is a hash of a concatenation of a nonce and a hash of a password. When the user requests access to the server, the server provides the user a nonce which is a randomly selected number. As the nonce changes each time access is requested, an eavesdropper would be unable to gain sufficient information with which to provide a second argument during a subsequent exchange between the eavesdropper and the server. To check the validity of the second argument, the server accesses a first term in the database, which is a first hash of the user's password, and concatenates the current nonce, R, to the value and applies a fourth hash to the result of the concatenation comparing the result to the second argument sent by the user.

Detailed Description Text (26):
Here, a first field 17a" of the table 15a" corresponds to a username or some identifying information. Typically, the identification information would be a user's first and/or last name or some combination thereof. The table 15a" includes a second field 17b" TERM.sub.-- 1 corresponding to an entry which is an encryption of a message where the message is a hash of a user's password, using a first hash function H.sub.1. The key under which the message is encrypted is a hash of a result of a concatenation between a hash of a user's password or other message, using a first hash function H.sub.1, and a nonce, the hash of the result of the concatenation using a second hash function H.sub.2. The contents of the second field 17b" is denoted as {H.sub.1 (pwd)}H.sub.2
(R.sub.1 .vertline..vertline.H.sub.1 (pwd)) where {H.sub.1 (pwd)} is encrypted

using the key H.sub.2 (R.sub.1 .vertline..vertline.H.sub.1 (pwd)). The table 15a" also includes a third field 17c" TERM.sub.-- 2 which corresponds to an entry which corresponds to a nonce, denoted as R.sub.1.

Detailed Description Text (27):
The contents of table 15a" are changed as a result of two different occurrences. The first occurrence is when a user, such as USER.sub.-- 1 10, changes its password, (pwd), new values are determined for TERM.sub.-- 1 17b" and TERM.sub.-- 2 17c" to reflect the change and table 15a" is updated with the new values.

Detailed Description Text (35):
The server checks the user's response by decrypting a first term in the server database using the first argument provided by the user. The result of the decryption, which is a first hash of the user's password, is used to verify the second argument by concatenating the result of the decryption to a second nonce and applying a third hashing function to the result of the concatenation. Once the response has been verified, the server generates a new first nonce and updates the contents of the database accordingly.

Detailed Description Text (37):
Here, a first field 17a'" of the table 15a'" corresponds to a username or some identifying information. Typically, the identification information would be a user's first and/or last name or some combination thereof. The table 15a'" includes a second field 17b'" corresponding to an entry which is an encryption of a message. Here, the message is a hash of a user's password or other message concatenated with a third nonce, using a first hash function H.sub.1. The key under which the message is encrypted is a hash of a result of a concatenation between a hash of a user's password or other message and a first nonce R.sub.1 where the user's password is first concatenated with a third nonce R.sub.3 before being hashed using a first hashing function H.sub.1. The contents of the second field 17b'" is denoted as {H.sub.1 (pwd.vertline..vertline.R.sub.3)}H.sub.2 (R.sub.1 .vertline..vertline.H.sub.1 (pwd.vertline..vertline.R.sub.3)) where {H.sub.1 (pwd.vertline..vertline.R.sub.3)} is encrypted using H.sub.2 (R.sub.1 .vertline..vertline.H.sub.1 (pwd.vertline..vertline.R.sub.3)) as a key. The table 15a'" also includes a third field 17c'", which corresponds to an entry which is a first nonce, denoted as R.sub.1 and a fourth field 17d'", which corresponds to an entry which is a third nonce, denoted as R.sub.3.

Detailed Description Text (38):
The contents of table 15a'" are updated as a result of three different occurrences. The first occurrence takes place when a user, such as USER.sub.-- 1 10, changes its password, (pwd). In response to the user selecting a new password, the server node 11 selects several pairs of a new first nonce, R.sub.1, and a new third nonce, R.sub.3. These nonce pairs and the new user password are used by the server node 11 to determine new values, called triplets, for the appropriate table 15a'" fields, 17b'", 17c'" and 17d'". One set of triplets is used to update the table 15a'" fields 17b'", 17c'" and 17d'". The remaining triplets are kept in reserve, that is stored somewhere separate from table 15a'" such that they are unlikely to be revealed even if table 15a'" is revealed. An example might be a backup tape of floppy disk stored in a safe. These remaining triplets are to be used if it is determined that table 15a'" has been compromised.

Current US Cross Reference Classification (1):
380/28

Current US Cross Reference Classification (2):
380/30

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 10 of 33 returned.

☐ 1. Document ID: US 20030120604 A1

Using default format because multiple data bases are involved.

L3: Entry 1 of 33 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

US-CL-CURRENT: 705/57; 705/400, 705/50

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 2. Document ID: US 20020107877 A1

L3: Entry 2 of 33 File: PGPB Aug 8, 2002

PGPUB-DOCUMENT-NUMBER: 20020107877
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020107877 A1

TITLE: SYSTEM FOR BACKING UP FILES FROM DISK VOLUMES ON MULTIPLE NODES OF A COMPUTER NETWORK

PUBLICATION-DATE: August 8, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
WHITING, DOUGLAS L.	CARLSBAD	CA	US	
DILATUSH, TOM	CHULA VISTA	CA	US	

US-CL-CURRENT: 707/204; 711/162

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 3. Document ID: US 20020077177 A1

L3: Entry 3 of 33 File: PGPB Jun 20, 2002

PGPUB-DOCUMENT-NUMBER: 20020077177
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020077177 A1

TITLE: SECURITY SYSTEM FOR VIDEO GAME SYSTEM WITH HARD DISK DRIVE AND INTERNET ACCESS CAPABILITY

PUBLICATION-DATE: June 20, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
ELLIOTT, SCOTT	REDMOND	WA	US	

US-CL-CURRENT: 463/40

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 4. Document ID: US 20020007452 A1

L3: Entry 4 of 33 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007452
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007452 A1

TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
TRAW, CHANDLER BRENDAN STANTON	PORTLAND	OR	US	
AUCSMITH, DAVID WAYNE	PORTLAND	OR	US	

US-CL-CURRENT: 713/152; 380/201, 705/57

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 5. Document ID: US 6859790 B1

L3: Entry 5 of 33 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 6. Document ID: US 6807024 B1

L3: Entry 6 of 33 File: USPT Oct 19, 2004

US-PAT-NO: 6807024
DOCUMENT-IDENTIFIER: US 6807024 B1

TITLE: Reproducing apparatus and reproducing method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 7. Document ID: US 6769061 B1

L3: Entry 7 of 33 File: USPT Jul 27, 2004

US-PAT-NO: 6769061
DOCUMENT-IDENTIFIER: US 6769061 B1

TITLE: Invisible encoding of meta-information

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 8. Document ID: US 6766305 B1

L3: Entry 8 of 33 File: USPT Jul 20, 2004

US-PAT-NO: 6766305
DOCUMENT-IDENTIFIER: US 6766305 B1
**** See image for Certificate of Correction ****

TITLE: Licensing system and method for freely distributed information

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 9. Document ID: US 6742028 B1

L3: Entry 9 of 33 File: USPT May 25, 2004

US-PAT-NO: 6742028
DOCUMENT-IDENTIFIER: US 6742028 B1

TITLE: Content management and sharing

Full | Title | Citation | Front | Review | Classification | Date | Reference | ... | Claims | KWIC | Draw De

☐ 10. Document ID: US 6592032 B1

L3: Entry 10 of 33 File: USPT Jul 15, 2003

US-PAT-NO: 6592032
DOCUMENT-IDENTIFIER: US 6592032 B1

TITLE: Control system and method of controlling information written into storage media

Full | Title | Citation | Front | Review | Classification | Date | Reference | ... | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L2 and @ad<=20001113	33

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 11 through 20 of 33 returned.

☐ 11. Document ID: US 6590588 B2

Using default format because multiple data bases are involved.

L3: Entry 11 of 33 File: USPT Jul 8, 2003

US-PAT-NO: 6590588
DOCUMENT-IDENTIFIER: US 6590588 B2

TITLE: Wireless, radio-frequency communications using a handheld computer

DATE-ISSUED: July 8, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Lincke; Scott D.	San Carlos	CA		
Marianetti, II; Ronald	Morgan Hill	CA		
Sipher; Joseph K.	Sunnyvale	CA		

US-CL-CURRENT: 715/744; 709/213, 709/218, 715/714, 715/763, 715/765, 715/835

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. De

☐ 12. Document ID: US 6560340 B1

L3: Entry 12 of 33 File: USPT May 6, 2003

US-PAT-NO: 6560340
DOCUMENT-IDENTIFIER: US 6560340 B1
** See image for Certificate of Correction **

TITLE: Method and apparatus for geographically limiting service in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw. De

☐ 13. Document ID: US 6542610 B2

L3: Entry 13 of 33 File: USPT Apr 1, 2003

US-PAT-NO: 6542610
DOCUMENT-IDENTIFIER: US 6542610 B2

TITLE: Content protection for digital transmission systems

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw. De

---

☐ 14. Document ID: US 6468160 B2

L3: Entry 14 of 33 File: USPT Oct 22, 2002

US-PAT-NO: 6468160
DOCUMENT-IDENTIFIER: US 6468160 B2
**** See image for Certificate of Correction ****

TITLE: Security system for video game system with hard disk drive and internet access capability

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw. De

---

☐ 15. Document ID: US 6463155 B1

L3: Entry 15 of 33 File: USPT Oct 8, 2002

US-PAT-NO: 6463155
DOCUMENT-IDENTIFIER: US 6463155 B1

TITLE: Broadcast reception device and contract management device using common master key in conditional access broadcast system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw. De

---

☐ 16. Document ID: US 6424717 B1

L3: Entry 16 of 33 File: USPT Jul 23, 2002

US-PAT-NO: 6424717
DOCUMENT-IDENTIFIER: US 6424717 B1
**** See image for Certificate of Correction ****

TITLE: Encryption devices for use in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWMC | Draw. De

---

☐ 17. Document ID: US 6421730 B1

L3: Entry 17 of 33 File: USPT Jul 16, 2002

US-PAT-NO: 6421730
DOCUMENT-IDENTIFIER: US 6421730 B1

TITLE: Programmable system for processing a partitioned network infrastructure

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 18. Document ID: US 6401117 B1

L3: Entry 18 of 33 File: USPT Jun 4, 2002

US-PAT-NO: 6401117
DOCUMENT-IDENTIFIER: US 6401117 B1
** See image for Certificate of Correction **

TITLE: Platform permitting execution of multiple network infrastructure applications

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 19. Document ID: US 6292568 B1

L3: Entry 19 of 33 File: USPT Sep 18, 2001

US-PAT-NO: 6292568
DOCUMENT-IDENTIFIER: US 6292568 B1
** See image for Certificate of Correction **

TITLE: Representing entitlements to service in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 20. Document ID: US 6252964 B1

L3: Entry 20 of 33 File: USPT Jun 26, 2001

US-PAT-NO: 6252964
DOCUMENT-IDENTIFIER: US 6252964 B1
** See image for Certificate of Correction **

TITLE: Authorization of services in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L2 and @ad<=20001113	33

Display Format: - Change Format

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 21 through 30 of 33 returned.

☐ 21. Document ID: US 6246767 B1

Using default format because multiple data bases are involved.

L3: Entry 21 of 33 File: USPT Jun 12, 2001

US-PAT-NO: 6246767
DOCUMENT-IDENTIFIER: US 6246767 B1
** See image for Certificate of Correction **

TITLE: Source authentication of download information in a conditional access system

DATE-ISSUED: June 12, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Akins, III; Glendon L.	Gainesville	GA		
Banker; Robert O.	Cumming	GA		
Palgon; Michael S.	Atlanta	GA		
Pinder; Howard G.	Norcross	GA		
Wasilewski; Anthony J.	Alpharetta	GA		

US-CL-CURRENT: 380/210; 380/232, 380/282, 380/285, 380/30, 380/43, 713/153, 713/168

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 22. Document ID: US 6195432 B1

L3: Entry 22 of 33 File: USPT Feb 27, 2001

US-PAT-NO: 6195432
DOCUMENT-IDENTIFIER: US 6195432 B1

TITLE: Software distribution system and software utilization scheme for improving security and user convenience

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 23. Document ID: US 6185683 B1

L3: Entry 23 of 33 File: USPT Feb 6, 2001

US-PAT-NO: 6185683
DOCUMENT-IDENTIFIER: US 6185683 B1
** See image for Certificate of Correction **

TITLE: Trusted and secure techniques, systems and methods for item delivery and execution

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 24. Document ID: US 6157955 A

L3: Entry 24 of 33 File: USPT Dec 5, 2000

US-PAT-NO: 6157955
DOCUMENT-IDENTIFIER: US 6157955 A
** See image for Certificate of Correction **

TITLE: Packet processing system including a policy engine having a classification unit

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 25. Document ID: US 6157719 A

L3: Entry 25 of 33 File: USPT Dec 5, 2000

US-PAT-NO: 6157719
DOCUMENT-IDENTIFIER: US 6157719 A
** See image for Certificate of Correction **

TITLE: Conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 26. Document ID: US 6144745 A

L3: Entry 26 of 33 File: USPT Nov 7, 2000

US-PAT-NO: 6144745
DOCUMENT-IDENTIFIER: US 6144745 A

TITLE: Method of and apparatus for retaining and verifying of data on recording medium

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

☐ 27. Document ID: US 6105134 A

L3: Entry 27 of 33 File: USPT Aug 15, 2000

US-PAT-NO: 6105134
DOCUMENT-IDENTIFIER: US 6105134 A

TITLE: Verification of the source of program information in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

☐ 28. Document ID: US 6076077 A

L3: Entry 28 of 33 File: USPT Jun 13, 2000

US-PAT-NO: 6076077
DOCUMENT-IDENTIFIER: US 6076077 A
** See image for Certificate of Correction **

TITLE: Data management system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

☐ 29. Document ID: US 5870473 A

L3: Entry 29 of 33 File: USPT Feb 9, 1999

US-PAT-NO: 5870473
DOCUMENT-IDENTIFIER: US 5870473 A

TITLE: Electronic transfer system and method

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

☐ 30. Document ID: US 5838790 A

L3: Entry 30 of 33 File: USPT Nov 17, 1998

US-PAT-NO: 5838790
DOCUMENT-IDENTIFIER: US 5838790 A
** See image for Certificate of Correction **

TITLE: Advertisement authentication system in which advertisements are downloaded for off-line display

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

---

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L2 and @ad<=20001113	33

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 31 through 33 of 33 returned.

☐ 31. Document ID: US 5802592 A

Using default format because multiple data bases are involved.

L3: Entry 31 of 33 File: USPT Sep 1, 1998

US-PAT-NO: 5802592
DOCUMENT-IDENTIFIER: US 5802592 A

TITLE: System and method for protecting integrity of alterable ROM using digital signatures

DATE-ISSUED: September 1, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Chess; David M.	Mohegan Lake	NY		
Sorkin; Gregory Bret	New York	NY		
White; Steve Richard	New York	NY		

US-CL-CURRENT: 711/164; 711/102, 711/103, 713/100, 713/2, 714/36, 714/38, 714/45

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 32. Document ID: US 5778395 A

L3: Entry 32 of 33 File: USPT Jul 7, 1998

US-PAT-NO: 5778395
DOCUMENT-IDENTIFIER: US 5778395 A

TITLE: System for backing up files from disk volumes on multiple nodes of a computer network

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 33. Document ID: US 5666415 A

L3: Entry 33 of 33 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L2 and @ad<=20001113	33

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 6 of 6 returned.

☐ 1. Document ID: US 20030120604 A1

Using default format because multiple data bases are involved.

L10: Entry 1 of 6 File: PGPB Jun 26, 2003

PGPUB-DOCUMENT-NUMBER: 20030120604
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20030120604 A1

TITLE: Reproducing apparatus and reproducing method

PUBLICATION-DATE: June 26, 2003

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Yokota, Teppei	Chiba		JP	
Kihara, Nobuyuki	Tokyo		JP	
Yamada, Eiichi	Tokyo		JP	
Okaue, Takumi	Kanagawa		JP	

US-CL-CURRENT: 705/57; 705/400, 705/50

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw. De

☐ 2. Document ID: US 20020007452 A1

L10: Entry 2 of 6 File: PGPB Jan 17, 2002

PGPUB-DOCUMENT-NUMBER: 20020007452
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020007452 A1

TITLE: CONTENT PROTECTION FOR DIGITAL TRANSMISSION SYSTEMS

PUBLICATION-DATE: January 17, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
TRAW, CHANDLER BRENDAN STANTON	PORTLAND	OR	US	
AUCSMITH, DAVID WAYNE	PORTLAND	OR	US	

US-CL-CURRENT: 713/152; 380/201, 705/57

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 3. Document ID: US 6859790 B1

L10: Entry 3 of 6 File: USPT Feb 22, 2005

US-PAT-NO: 6859790
DOCUMENT-IDENTIFIER: US 6859790 B1

TITLE: Data distribution system and method thereof, data processing device, data control device, and machine-readable recording medium recording distribution data

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 4. Document ID: US 6246767 B1

L10: Entry 4 of 6 File: USPT Jun 12, 2001

US-PAT-NO: 6246767
DOCUMENT-IDENTIFIER: US 6246767 B1
** See image for Certificate of Correction **

TITLE: Source authentication of download information in a conditional access system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 5. Document ID: US 6076077 A

L10: Entry 5 of 6 File: USPT Jun 13, 2000

US-PAT-NO: 6076077
DOCUMENT-IDENTIFIER: US 6076077 A
** See image for Certificate of Correction **

TITLE: Data management system

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw De

☐ 6. Document ID: US 5666415 A

L10: Entry 6 of 6 File: USPT Sep 9, 1997

US-PAT-NO: 5666415
DOCUMENT-IDENTIFIER: US 5666415 A

TITLE: Method and apparatus for cryptographic authentication

Full | Title | Citation | Front | Review | Classification | Date | Reference | Claims | KWIC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L9 and L3	6

Display Format: - Change Format

Previous Page Next Page Go to Doc#